Maulana Abul Kalam Azad University of Technology, West Bengal

(Formerly West Bengal University of Technology)

Syllabus for M. Sc. (Information & Cyber Security)

(Effective for Academic Session 2019-2020)

Curriculum Structure

Year	Semester	Paper Code	Paper	Marks	Credit
1	1	MICS101	Discrete Mathematics	100	4
		MICS102	Linear Algebra	100	4
		MICS103	Computer Networks	100	4
		MICS104	Design and Analysis of Algorithms	100	4
		MICS191	Python Programming Lab	100	3
		MICS192	Design and Analysis of Algorithms Lab	100	3
				600	22

Year	Semester	Paper Code	Paper	Marks	Credit
1	2	MICS201	Cryptography	100	4
		MICS202	Operating Systems	100	4
		MICS203	Bayesian Networks	100	4
		MICS204	Pattern Recognition and Machine Learning	100	4
		MICS205	Network Security Firewalls and Virtual Private Networks	100	4
		MICS291	Machine Learning Lab	100	3
		MICS292	Operating Systems Lab	100	3
				700	26

Year	Semester	Paper Code	Paper	Marks	Credit
2	3	MICS301	Information Security Risk Management	100	4
		MICS302	Biometric Security	100	4
		MICS303	Data Privacy	100	4
		MICS304	Intrusion Detection and Prevention Systems	100	4
		MICS305	Wireless and Mobile Device Security	100	4
		MICS391	Linux Systems Security Lab	100	3
		MICS392	Wireless Security Lab	100	3
				700	26

Maulana Abul Kalam Azad University of Technology, West Bengal

(Formerly West Bengal University of Technology)

Syllabus for M. Sc. (Information & Cyber Security)

(Effective for Academic Session 2019-2020)

Year	Semester	Paper Code	Paper	Marks	Credit
2	4		Elective I	100	4
			Elective II	100	4
		MICS481	Major Project	100	8
		MICS 482	Grand Viva	100	6
				400	22

Elective Set	Course Code	Topic
I	MICS-E401A	Security in Internet of Things
	MICS-E401B	Security in Cloud Computing
	MICS-E401C	Legal Issues in Cyber Security
II	MICS-E402A	Computer Forensics
	MICS-E402B	Information Warfare
	MICS-E402C	Social Network Analysis

Semester No	Total Credit
1	22
2	26
3	26
4	22
Total	96

Maulana Abul Kalam Azad University of Technology, West Bengal

(Formerly West Bengal University of Technology)

Syllabus for M. Sc. (Information & Cyber Security)

(Effective for Academic Session 2019-2020)

Semester 1

Discrete Mathematics

Set Theory: Definition of Sets, Venn Diagrams, complements, cartesian products, power sets, counting principle, cardinality and countability (Countable and Uncountable sets), Relation: Definition, types of relation, composition of relations, domain and range of a relation, pictorial representation of relation, properties of relation, partial ordering relation, Function, Definition and types of function, composition of functions, recursively defined functions Propositional logic, Proposition logic, basic logic, logical connectives, truth tables, tautologies, contradiction , normal forms(conjunctive and disjunctive), modus ponens and modus tollens, validity, predicate logic, universal and existential quantification. Notion of proof: proof by implication, converse, inverse, contrapositive, negation, and contradiction, direct proof, proof by using truth table, proof by counter example, Logical equivalence, Permutation and combinations, Generating functions, Recurrence relations, Combinatories: Mathematical induction, recursive mathematical definitions, basics of counting, permutations, combinations, inclusion-exclusion, recurrence relations, generating function ,Algebraic Structure: Binary composition and its properties definition of algebraic structure; Groyas Semigroup, Monoid Groups, Abelian Group, properties of groups, Permutation Groups, Sub Group, Cyclic Group, Rings and Fields (definition and standard results). Graph : terminology, types of graph connected graphs, components of graph, Euler graph, Hamiltonian path and circuits, Graph coloring, Chromatic number, sub-graphs, cyclic graphs, Tree: Definition, types of tree(rooted, binary), properties of trees, binary search tree, tree traversing (preorder, inorder, postorder), spanning trees, binary trees, Algorithms- Kruskal's , Prim's , Dijkstra's , Flyod's , Warshall's, DFS, BFS, Isomorphism, homomorphism , Finite Automata: Basic concepts of Automation theory, Deterministic finite, NFA, DFA, Conversion, Mealy M/C, Moore M/C, Introduction to Languages & Grammars and their relation with Automata

Text Books:

1. Kenneth H. Rosen, "Discrete Mathematics and its Applications", Mc.Graw Hill.

2. J.P.Tremblay & R. Manohar, "Discrete Mathematical Structure with Applications

3. Mott, Kandel & Baker, PHI, Discrete Mathematics for Comp. Scientists & Mathematicians

4. C.L.Liu, . Discrete Mathematical Structure ,TMH

4. G.S.Rao, Discrete Mathematical Structure

Linear Algebra

Systems of linear equations, Equivalent Systems of Linear Equations, Inverses of Elementary Row-operations,Matrices, Elementary and Invertible Matrices, Homogeneous and Non-homogeneous Equations, Elementary row operations, Row-reduced echelon matrices. Vector spaces, Subspaces, Bases and dimension, Dimension of a vector space, Ordered bases and coordinates.
Linear transformations, Null Space and the Range Space, Rank-nullity theorem, Algebra of linear transformations, Isomorphism, Matrix representation, Linear functionals, Annihilator, Double dual, Transpose of a linear transformation. Eigenvalues and Eigenvectors of Linear Operators, Characteristic values and characteristic vectors of linear transformations, Diagonalizability, Minimal polynomial of a linear transformation, Cayley-Hamilton theorem, Invariant subspaces, Triangulability, Diagonalization in Terms of the Minimal Polynomial, Independent Subspaces and Projection Operators,
Direct-sum decompositions, Invariant direct sums, The primary decomposition theorem, Cyclic subspaces and annihilators, The Cyclic Decomposition Theorem, Inner Product Spaces, Rational, Jordan forms, Orthonormal bases, Gram-Schmidt process, Bessel's Inequality, Parseval's Indentity, Best Approximation, The Adjoint Operator, Unitary Operators, Self-Adjoint Operators, Normal Operators - Spectral Theorem

Text Books:
1. K.Hoffman and R. Kunze, Linear Algebra, 2nd Edition, Prentice- Hall of India

2. M. Artin, Algebra, Prentice-Hall of India

Computer Networks

Fundamentals of data transmission, wired and wireless media, digital and analog transmission, data coding techniques, multiplexing, overview on OSI layers and TCP/IP model, Local Area Networks and data link protocols, point-to-point links and sliding window flow control, CSMA/CD, Ethernet, wireless LAN, cellular networks, and advanced multi-user communication (CDMA, SDMA/MIMO), mobility Internetworking using TCP/IP: network programming using socket API, network client/server design, Packet/circuit switching and wide-area networks: store-and-forward networks, source routing, virtual/permanent, circuits and call set-up, LAN/WAN addressing, hop-by-hop vs. end-to-end control, Routing techniques - intra-domain routing (OSPF, RIP), inter-domain policy routing (BGP) and network connectivity Transport protocols - TCP and UDP, Congestion control, TCP window control, multimedia Streaming, High-level network services - DNS, HTTP, SMTP, network management (SNMP), network Security

Text Books:

1.Computer Networks by AS Tanenbaum, Pearson Education

2. Data Communication and Networking by B. Forouzan

3. Data and Communication by W. Stallings

Design and Analysis of Algorithm

Basic Computational Model and analyzing Algorithms, Asymptotic Notation and recurrence relations, Fundamental design methodologies and their implementations: Dynamics Programming, Greedy algorithms, Divide and Conquer, Branch and Bound, Prune-and-Search , Backtracking, Randomized Techniques, Algorithms for set manipulations, their implementations and applications: Union-Find, Priority Queues. Graph Algorithms with implementation issues; Breadth First and Depth-First Search and their applications, Minimum Spanning Trees and Shortest Paths, Graph Search, Matrix Multiplication, Pattern Matching, Polynomial Arithmetic and FFT, Introduction to the Theory of Lower Bounds, NP-Completeness and Reductions

Text Books:

1. E. Horowitz & S. Sahani : Fundamental of Computer Algorithm (Galgotia)

2. Coreman, Leiserson & Rivest : Introduction to Algorithm (MIT)

3. Brassard & Brately : Algorithm- Theory and Practice (PHI)

Python Programming Lab

Manipulating strings, Processing Files, Manipulating Lists, Lists and Strings, Dictionarys, Counting with Dictionaries, Dictionaries and Files, Tuples, Tuples and Sorting, Regular Expressions, Networked programs, Sockets and Applications, parsing HTML with Beautifulsoup, parsing XML by python, REST,JSON and APIs, Extracting data from JSON, Using database by python, Object oriented python, Geocoding, Page rank and web searching, Gmane

Design and Analysis of Algorithms Lab

analyze a problem & design the solution for the problem in matrix multiplication, Prim's algorithm, Kruskal's algorithm using dynamic programming method, Huffman's algorithm, all pairs shortest path problem, file compression (and un-compression) using Huffman's algorithm ,0/1 knapsack problem using Greedy algorithm , Dynamic programming algorithm , Backtracking algorithm, Branch and bound algorithm, optimal binary search tree problem , traveling sales persons problem using Dynamic programming algorithm , back tracking algorithm., Branch and Bound method

Semester 2

Cryptography

Number Theory; Mathematics of Secure Communications; Classical Cryptosystems; Knapsack Problem, Public key Cryptosystems RSA and other Cryptosystems, Key Exchange Protocols, Hash Functions, Digital Signatures, Digital Certificates, Elementary Concepts of Coding Theory; Applications of Algebraic Coding Theory to Cryptography, Recent Advances in Cryptology , Private Key Cryptosystems, Modern techniques, algorithms like DES, AES, IDEA, RC5, Blow fish etc; Elliptic curves: Theory and Applications to Factorization and Cryptography

Text Books:

1. William Stallings: Cryptography and Network security, Pearson Education

2. Alfred Menezes: Handbook of Applied Cryptography.

3. Wenbo Mao: Modern Cryptography: Theory and Practice, Pearson Education

Operating System

OS services and components, multitasking, multiprogramming, time sharing, buffering, Spooling Process & thread management, context switching, multithreading, Concurrency control, mutual exclusion requirements, semaphores, monitors, Dead-locks - detection, recovery, avoidance and prevention, Memory management, partitioning, swapping, paging, segmentation, virtual memory,Demand paging, page replacement and allocation algorithm, Introduction to Distributed Systems, Architectures of Distributed Systems, Communication networks, Mutual Exclusion in Distributed Systems, RMI, concept of Replication, Distributed File Systems (NFS, AFS, coda) overview, security in Distributed Systems. HDFS File and Storage Management

Text Books:

1. Advanced Concepts in Operating Systems by Mukesh Singhal and Niranjan Shivaratri

2. Distributed Operating systems by Andrew S. Tanenbanm

3. Operating System Concepts, by Silberschatz and Galvin

Bayesian Networks

Representation, Independence and conditional independence, Partial independence and other structure, Exact inference in BBN, Variable elimination, Pearl's algorithm, Junction tree, Recursive decomposition Using additional structure, Approximate inference, Monte Carlo approximations, Loopy belief propagation, Variational methods, Learning of BBNs, learning parameters, learning structure, Bayesian averaging, EM (learning with hidden variables and missing values), structural EM, Dynamic belief networks, Particle filtering, Markov random fields (Markov networks) Representation (potentials), Independence and conditional independence, Trees, Boltzman machines, Conditional Markov random fields, Inference in Markov networks, Learning Markov networks:, Iterative proportional fitting, Cluster variational methods, Other approximations, Relational graphical models

Text Books:

1.Judea Pearl. Probabilistic Reasoning in Intelligent Systems. Morgan Kaufman.

2. Finn Jensen. An introduction to Bayesian Networks. Springer-Verlag.

3. S. Lauritzen. Graphical Models. Oxford University Press.

4. David J.C. Mackay. Information theory, inference, and learning algorithms. Cambridge, UK:Cambridge University Press.

5. Michael Jordan. Introduction to Graphical Models

6. Daphne Koller and Nir Friedman. Bayesian Networks and Beyond

Pattern Recognition and Machine Learning

Introduction: Data Mining Concept, Origin, Process, Applications, Techniques, Challenges
Data Preprocessing: Data types, Quality, Descriptive data summarization – central tendency and dispersion measure, Data cleaning, Data integration & transform, Data reduction
Association Rule Mining: Market-basket analysis basics, Naïve algorithm, Apriori algorithm, Direct Hashing and Pruning (DHP), Software for Association Rule Mining
Classification and Prediction: Decision Tree, Classification by decision tree induction,
Bayesian classification, Rule-based classification, Prediction – Linear and Nonlinear
Regression, Classification software
Supervised Learning, Decision Tree, Linear Discriminant Functions , Support Vector Machine (SVM)
Neural Network, Deep belief network, Density elimination Methods
Bayes Decision Theory, Expectation and Minimization , Ensemble Methods, Feature Engineering
Cluster Analysis: Types of data in cluster analysis, Partitioning methods, Hierarchical methods, Density-based methods, Quality & Validity of clustering methods , Cluster analysis software
Web Data Mining: Web content mining, Web usage mining, Web structure mining, Hubs and Authorities, HITS algorithm, Web mining software , Text Mining, Support Vector Machine.
Data Mining Application & Information Privacy: Applications and trends in data mining such as Web, finance, telecommunication, biology and medicine, science and engineering retail industry etc. Social impacts of data mining, information privacy and data security, IT Act overview.

Text Books:

1. Tan, Steinbach and Kumar, Introduction to Data Mining, Pearson
2. Han and Camber, Data Mining: Concepts and Techniques, Morgan Kaufmann
3. Foreman, Data Smart:Using Data Science to Transform Information into Insight
4. Machine Learning and Knowledge Discovery edited by Walter Daelemans, Katharina Morik
5. Pattern Recognition and Machine Learning by Christopher Bishop
6. Introduction to Machine learning with python by Andreas C. Müller and Sarah Guido John Wiley
7. Dunham, Data Mining : Introductory and Advanced Topics, Pearson

Network Security Firewalls and Virtual Private Networks

Introduction , Fundamentals of Network Security, Threats and issues, Information and network security iterms, concepts, threats and common attacks, Network Security Implementation and management , Security Policies and Standards, Key information security management practices , Authenticating Users : critical aspect of perimeter defence mechanism, process of firewall authentication , advantages and disadvantages of popular centralized authentication systems,
Control Hijacking– Attacks and defenses, Buffer overflow and control hijacking attacks
Exploitation techniques and fuzzing- Finding vulnerabilities and exploits
Dealing with Legacy code- Dealing with bad (legacy) application code: Sandboxing and Isolation.
Least privilege, access control, operating system security- The principle of least privilege, Access control concepts, Operating system mechanisms, Unix, Windows, Qmail, Chromium, and Android examples.
Basic web security model- Browser content, Document object model (DOM), Same-origin policy.
Web Application Security- SQL injection, Cross-site request forgery, Cross-site scripting, Attacks and Defenses, Generating and storing session tokens, Authenticating users, The SSL protocol, The lock icon, User interface attacks, Pretty Good Privacy
Firewalls : cardinal activities and types of protection, features and common misconceptions
Packets and Packet Filtering : specific filtering rules based on business needs,
Firewall Fundamentals, Types, Configuration and Administration , Identification and implementation of different firewall configuration strategies, Firewall Deployment Considerations,
Security principles for firewall, security strategies, Firewall Management and Security Concerns , Tracking firewall log files , Following the basic initial steps in responding to security incidents
Proxy Servers and Application-Level Firewalls, Functions and configurations, situations when proxy server is not the correct choice,
Implementing Bastion Host :general requirements for installing a bastion host, Evaluation for different options for positioning the bastion host (physically and within the network), baseline performance level and audit procedures, Firewall Implementation Planning,
Encryption – VPN Fundamentals, Foundation for the Virtual Private Network : encryption role in firewall and VPN architectures, VPN Management : Policy and Best Practices
VPN Technologies, Improving VPN Performance and Stability, Firewall Implementation
Real-World VPNs, Attacking a Virtual Private Network, Perspectives, Resources, and the Future, Investigating and Responding to Security Incidents
Internet Protocol Security (IPSec) : its protocols and modes

Text Books:

1. William Stallings, Network Security Essentials: Applications and Standards, Prentice Hall, 4th edition, 2010.
2. Michael T. Goodrich and Roberto Tamassia, Introduction to Computer Security, Addison Wesley, 2011.
3. William Stallings, Network Security Essentials: Applications and Standards, Prentice Hall, 4th edition, 2010
4. Michael E. Whitman, Herbert J. Mattford, and Andrew Green: Guide to Firewalls and VPNs (ISBN: 978-1-111-13539-3), Course Technology / Cengage Learning
5. Stewart: Network Security, Firewalls, and VPNs

Machine Learning Lab

Implement and demonstrate the decision tree based ID3 algorithm, Artificial Neural Network by implementing the Back-propagation algorithm , naïve Bayesian classifier , naïve Bayesian Classifier model , Bayesian network, k-Means algorithm, Ensemble Methods, Feature Engineering , Association Rule Mining

Operatng System Lab

Shell Programming-creating a script, making a script executable, shell syntax (variables, conditions, control structures, functions, commands).
Process-starting a process, conditions, control structures, functions, commands),waiting for a process, zombie process Semaphore-programming with Semaphore

Semester 3

Information Security Risk Management

An Introduction to Risk Management: Introduction to the Theories of Risk Management; The Changing Environment; The Art of Managing Risks. The Threat Assessment Process: Threat Assessment and its Input to Risk Assessment; Threat Assessment Method; Example Threat Assessment; Vulnerability Issues: Operating System Vulnerabilities; Application Vulnerabilities; Public Domain or Commercial Off-the-Shelf Software; Connectivity and Dependence; Vulnerability assessment for natural disaster, technological hazards, and terrorist threats; implications for emergency response, vulnerability of critical infrastructures; The Risk Process: What is Risk Assessment? Risk Analysis; Who is Responsible? Tools and Types of Risk Assessment: Qualitative and Quantitative risk Assessment; Policies, Procedures, Plans, and Processes of Risk Management; Tools and Techniques; Integrated Risk Management; Future Directions: The Future of the Risk Management

Text books:

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

Biometric Security

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

Text Books:

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

Data Privacy

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

Text Books:

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

Intrusion Detection and Prevention Systems

History of Intrusion detection, Audit, Concept and definition , Internal and external threats to data, attacks, Need and types of IDS, Information sources Host based information sources, Network based information sources.
The state of threats against computers, and networked systems, Overview of computer security solutions and failure causes, Vulnerability assessment, firewalls, Overview of Intrusion Detection and Intrusion Prevention, Network and Host-based IDS,
Evaluation of IDS, Cost sensitive IDS, Anomaly Detection Systems and Algorithms, Network Behavior Based Anomaly Detectors (rate based), Host-based Anomaly Detectors
Intrusion Prevention Systems, Network IDs protocol based IDs ,Hybrid IDs, Analysis schemes, thinking about intrusion. A model for intrusion analysis , techniques,
Classes of attacks, Network layer attack (scans, denial of service, penetration), Application layer attack(software exploits, code injection), Human layer attack (identity theft, root access),
Responses requirement of responses, types of responses mapping responses to policy Vulnerability analysis, credential analysis non credential analysis,
Automated: Drones, Worms, Viruses, A General IDS model and taxonomy, Signature-based Solutions, Introduction to Snort, Snort rules , Snort Installation Scenarios, Installing Snort, Running Snort on Multiple Network Interfaces, Snort Command Line Options. Step-By-Step Procedure to Compile and Install Snort Location of Snort Files, Snort Modes Snort Alert Modes,
State transition, Immunology, Payload Anomaly Detection, Attack trees and Correlation of alerts, Autopsy of Worms and Botnets, Malware detection
Working with Snort Rules, Rule Headers, Rule Options, The Snort Configuration File etc. Plugins, Preprocessors and Output Modules, Using Snort with MySQL,
Email/IM security issues, Viruses/Spam, From signatures to thumbprints to zero-day detection, Insider Threat issues , Masquerade and Impersonation, Traitors, Decoys and Deception
Using ACID and Snort Snarf with Snort, Agent development for intrusion detection, Architecture models of IDs and IPs

Text Books:

1. Rafeeq Rehman : " Intrusion Detection with SNORT, Apache, MySQL, PHP and ACID," Prentice Hall
2. Christopher Kruegel,Fredrik Valeur, Giovanni Vigna: "Intrusion Detection and Correlation Challenges and Solutions",
3. Carl Endorf, Eugene Schultz and Jim Mellander " Intrusion Detection & Prevention", Tata McGraw-Hill
4. Stephen Northcutt, Judy Novak : "Network Intrusion Detection", New Riders Publishing
5. T. Fahringer, R. Prodan, "A Text book on Grid Application
Development and Computing Environment". Khanna Publihsers

Wireless and Mobile Device Security

Mobile Computing Overview, Wired/wireless networks; Effect of mobility on networks and systems; impact on IP stack from MAC layer and up; ad-hoc and sensor networks; wireless broadcast , Wireless Communications Infrastructure Vulnerabilities, Wireless Communications Infrastructure Vulnerabilities Mitigation Techniques, Introduction to Mobile Security, Building Blocks – Basic security and cryptographic techniques ,
, IP broadcast, Satellite broadcast; issues of information capacity; distinction between wired and wireless networks from information theory; Issues of security in wireless; issues of 802.11 protocols; routing in wireless networks, design of secure protocols: key distribution for access control, source authentication of transmissions, and non-repudiation; Power management and selfishness issues, attacks in wireless networks; DoS and DDoS attacks, reaction to attacks, information processing for sensor networks ,
Mobile Platform Vulnerabilities, Mobile Platform Vulnerabilities Mitigation Techniques, Mobile App Vulnerabilities, Mobile App Vulnerabilities Mitigation Techniques, Mobile Device Vulnerabilities, Mobile Device Vulnerabilities Mitigation Techniques and Organizational Mobile Device Security Policy Requirements
Security of GSM Networks, Security of UMTS Networks , LTE Security, WiFi and Bluetooth Security, SIM/UICC Security, Mobile Malware and App Security, Android Security Model, IOS Security Model, Security Model of the Windows Phone, SMS/MMS, Mobile Geolocation and Mobile Web Security, Security of Mobile VoIP Communications, Emerging Trends in Mobile Security

Text Books

1. Lei Chen, Jiahuang Ji, Zihong Zhang, Wireless Network Security, Springer Science & Business Media,2013
2. Noureddine Boudriga, Security of Mobile Communications, 2010
3. Mobile Application Security, Himanshu Dviwedi, Chris Clark and David Thiel
4. Security of Mobile Communications, Noureddine Boudriga

Linux System Security Lab

Attacks against Linux: Exploits and Vulnerabilities - Weak passwords, suid binaries, Buffer overflow, Race conditions, Key logging

Trojans and Backdoors: The Sendmail Torjan, Modifying /etc/passwd, Modifying /etc/inetd.cof, Creating suid shells, Trojaned System binaries, CGI abuse.

Rootkits: FLEA, TOrn, Adore

Denial of Service: Ping-Pong attack, Ditributed Flood Nets, The Smurf attack, Fragmentation attack, SYN flooding, nonbandwidth-oriented DoS attacks

TCP/IP Attaks: ARP Spoofing, DNS ttacks, Packet Sniffing, Switched LAN Sniffing, IP Spoofing, Man-in-the-Middle Attack, Replay attack, Injection attacks.

Assessing the Network: Portscanning with Nmap, Vulnerability auditing with Nessus, Website auditing with Nikto

Packet Filtering with IPtables: The components of an Iptable Rule, Generic matches, TCP-specific matches, UDP-specific matches, UDP-specific matches, ICMP-specific matches, Matching extensions, Targets.

Creating a Firewall ruleset: Protecting the Firewall, Protecting the DMZ, ICMP messages, TTL rewriting, Blocking unwanted hosts, Filtering illegal addresses, Local packet filtering.

Firewall Management: dealing with dynamic IP address DHCPED, blocking and unblocking hosts, Using CGI management tools.

Access Control: Role-based access control with Grsecurity, Linux Intrusion Detection Systems, SeLinux, DTE,

Securing Web Services - SSH, NFS and NIS, DNS and BIND, Securing FTP,

Wireless Security Lab

IEEE 802.11 Standard

Lab 1: Selfish Behavior in Wireless Networks: Configuration of wireless client adaptors, How much do we get out of the 11 MBPS in IEEE 802.11b?

Lab 2: Unauthorized Access in Wireless Networks: Hacking MAC filtering, Cracking the WEP encryption, Breaking WPA2 Personal Passwords

Lab 3: Global Positioning System and DSSS: Global Positioning System, Speed Spectrum Techniques: Direct Sequence Spread Spectrum (DSSS)

Lab 4: Jamming Resistant Communication: Jamming in Wireless Networks - Attacking Team, Monitoring Team.

Lab 5: MAC Spoofing and Detection

Lab 6: ARP Cache Poisoning and Defence

Lab 7: WEP Key Cracking and Decryption

Lab 8: Isolating WLAN traffic using Firewalls for VPN connection

Semester 4

Elective Set I:

Security in Internet of Things

Internet of Things (IOT): Internet in general and Internet of Things, IoT architectures: layers, protocols, packets, services, performance parameters of a packet network as well as applications such as web, Peer-to-peer, sensor networks, and multimedia, IoT enabling technologies, IoT Big Data Analytics, IoT security and privacy concerns.
Computing paradigms: Virtualization Vulnerabilities, Hypervisor Security-Related Issues, Side Channel Attacks, Data Segregation, ubiquitous, grid, cloud, pervasive, green, ad hoc (*mobile*, *vehicular*, *flying*) networks.
Spear Phishing: Advanced Persistent Threats, Reconnaissance.
Digital Rights Management (DRM): Usage Rights, Rights Expression Language, Open Digital Rights Language.
Android-based Smartphone Security, Stepping Stone Detection, Broken Authentication and Session Management Vulnerabilities, Computer Forensic Investigation, Cyber Terrorism

Text Books:

1. Gunter Ollmann 2007. The Phishing Guide Understanding & Preventing Phishing Attacks. IBM Internet Security Systems.

2. Thomas Erl, Ricardo Puttini, ZaighamMahmood, Cloud Computing: Concepts, Technology & Architecture, Prentice Hall, 2013.

3. RajkumarBuyya, Christian Vecchiola, S. ThamaraiSelvi, Mastering Cloud Computing, Tata McGraw-Hill Education, 2013.

Security in Cloud Computing

Cloud Computing Fundamentals: What Cloud Computing, Essential Characteristics, Architectural Influences, Technological Influences. Cloud Computing Architecture: Cloud Delivery Models, Cloud Deployment Models, Expected Benefits. Cloud Computing Software Security Fundamentals: Cloud Information Security Objectives, Cloud Security Services, Relevant Cloud Security Design Principles, Secure Cloud Software Requirements. Cloud Computing Risk Issues: Privacy and Compliance Risks, Threats to Infrastructure, Data, and Access Control, Cloud Service Provider Risks, Cloud Computing Security Challenges: Security Policy Implementation, Virtualization Security Management, VM Security Recommendations, VM-Specific Security Techniques. Cloud Computing Security Architecture: Architectural Considerations, Identity Management and Access Control, Autonomic Security. Data storage in the cloud: Understanding cloud-based data storage, cloud-based backup system, Understanding File storage, Industry specific cloud-based data storage, Cloud-based database solutions, Cloud-based block storage. Collaboration in the cloud: Web based collaborations, Collaborating via web Logs(Blogs), Using social media for collaboration, Using streaming video content to collaborate.

Text Books:

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

Legal Issues in Cyber Security

Introduction-Cyber Security and its problem-Intervention Strategies: Redundancy, Diversity and Autarchy. Introduction to the Legal Perspectives of Cybercrimes and Cyber security, Cybercrime and the Legal Landscape around the World, Why Do We Need Cyber laws, The Indian IT Act, Challenges to Indian Law and Cybercrime Scenario in India, Consequences of Not Addressing the Weakness in Information Technology Act, Digital Signatures and the Indian IT Act, Cybercrime and Punishment, Cyber law, Technology and Students: Indian Scenario. Private ordering solutions, Regulation and Jurisdiction for global Cyber security, Copy Right-source of risks, Pirates, Internet Infringement, Fair Use, postings, criminal liability, First Amendments, Data Losing. Ethics, Legal Developments, Cyber security in Society, Security in cyber laws case studies, General lawand Cyber Law-a Swift Analysis

Text books:

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

Elective Set II:

Computer Forensics

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

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

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

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

Text Books:

1. Jason Luttgens, Matthew Pepe, Kevin Mandia, Incident Response & Computer Forensics, McGraw-Hill Osborne Media, 3rd edition , 2014.

2. Keith J. Jones, Richard Bejtlich, Curtis W. Rose, Real Digital Forensics: Computer Security and Incident Response, Paperback – Import, 2005.

Information Warfare

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

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

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

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

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

Text books:

1. Daniel Ventre, Cyberwar and Information Warfare, John Wiley & Sons.2012

2. Daniel Ventre, Information Warfare, Wiley - ISTE (2009)

Social Network Analysis

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

Random network models: Erdos-Renyi and Barabasi-Albert- Concepts: connected components, giant component, average shortest path, diameter, breadth-first search, preferential attachment Network centrality- Concepts: Betweenness, closeness, eigenvector centrality (+ PageRank), network centralization

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

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

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

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

Text books:

1. John Scott, Social Network Analysis, 3rd Edition, SAGE, 2012.

2. Wouter de Nooy, Andrej Mrvar, Vladimir Batagelj, Exploratory Social Network Analysis with Pajek, 2nd Revised Edition, Cambridge University Press, 2011.

3. Patrick Doreian, Frans Stokman, Evolution of Social Networks, Routledge, 2013.

4. David Easley and Jon Kleinberg, Networks, Crowds, and Markets: Reasoning About a Highly Connected World, Cambridge University Press, 2010.