M. TECH - CYBER SECURITY

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

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

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

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

CURRICULUM

First Semester

Course Code	Type	Course	L T P	Cr
18MA603	FC	Mathematical Foundations for Cyber Security	3 1 0	4
18CY601	FC	Concepts in System Security	3 0 0	3
18CY602	FC	Cryptography	3 0 2	4
18CY621	SC	Internet Protocols	3 0 0	3
	E	Elective 1	2 0 2	3
18HU601	HU	Amrita Values Program *		P/F
18HU602	HU	Career Competency I *		P/F
			Credits	**17**

* Non-Credit Course

Second Semester

Course Code	Type	Course	L T P	Cr
18CY622	SC	Cyber Forensics	2 0 2	3
18CY623	SC	Applied Cryptography	3 0 0	3
18CY603	FC	Secure Coding	2 0 2	3
18CY624	SC	Network Security	2 0 2	3
	E	Elective II	2 0 2	3
18CY625	SC	Cyber Security Lab	0 0 6	3
18HU603	HU	Career Competency II	1 0 0	1
18RM600	SC	Research Methodology	2 0 0	2
			Credits	**21**

Third Semester

Course Code	Type	Course	L T P	Cr
	E	Elective III	2 0 2	3
	E	Elective IV	2 0 2	3
18CY798	P	Dissertation		8
			Credits	**14**

Fourth Semester

Course Code	Type	Course	L T P	Cr
18CY799	P	Dissertation		12
			Credits	**12**

Total Credits: 64

List of Courses

Foundation Core

Course Code	Course	L T P	Cr
18MA603	Mathematical Foundations for Cyber Security	3 1 0	4
18CY601	Concepts in System Security	3 0 0	3
18CY602	Cryptography	3 0 2	4
18CY603	Secure Coding	2 0 2	3

Subject Core

Course Code	Course	L T P	Cr
18CY621	Internet Protocols	3 0 0	3
18CY622	Cyber Forensics	2 0 2	3
18CY623	Applied Cryptography	3 0 0	3
18CY624	Network Security	2 0 2	3
18CY625	Cyber Security Lab	0 0 6	3
18RM600	Research Methodology	2 0 0	2

Electives

Course Code	Course	L T P	Cr
	Elective I		
18CY701	Data Mining and Machine Learning in Cyber Security	2 0 2	3
18CY702	Distributed and Cloud Computing	2 0 2	3
18CY703	Design and Analysis of Algorithms	2 0 2	3
	Elective II		
18CY704	Wireless Networking and Security	2 0 2	3
18CY705	Coding and Information Theory	2 0 2	3
18CY706	Cryptographic Hardware and Embedded Systems	2 0 2	3
	Elective III		
18CY707	Steganography and Obfuscation	2 0 2	3
18CY708	Formal Methods for Security	2 0 2	3
18CY709	Android Security	2 0 2	3
	Elective IV		
18CY710	Security in Cloud Computing	2 0 2	3
18CY711	Special Topics in Cryptography	2 0 2	3
18CY712	Blockchain Technology	2 0 2	3
18CY713	Secure Systems Engineering	2 0 2	3

Project

Course Code	Courses	L T P	Cr
18CY798	Dissertation		8
18CY799	Dissertation		12

18MA603 MATHEMATICAL FOUNDATIONS FOR CYBER SECURITY 3-1-0-4

Elementary Number Theory – Divisibility, Prime numbers, Arithmetic functions, Congruence, Quadratic Residues, Primitive roots, Algorithms for primality testing, Integer Factorization and Discrete Logarithm. Algebraic Structures - Groups, Rings, Fields and Lattices. Polynomials over Finite Field – Order of Polynomials, Primitive polynomials, Extension Fields, Vector space, Subspace, Inner product space, Orthogonalization, Diagonalization, Arithmetic of Elliptic Curves, Bilinear maps, Solving nonlinear system of equations using XL algorithm and Grobner basis techniques.

TEXT BOOKS/REFERENCES:

1. R. Lidl and H. Niederreiter, *Finite Fields*, 2nd Edition, Cambridge University Press, 1997.
2. S.Y. Yan, *Number Theory for Computing*, 2nd Edition, Springer, Berlin, 2002.
3. G. Strang, *Introduction to Linear Algebra*, 4th Edition, Wellesley-Cambridge Press, 2009.
4. J. H . Silverman, *The Arithmetic of Elliptic Curves*, Vol. 106, Dordrecht: Springer, 2009.
5. A. Joux, *Algorithmic Cryptanalysis*, Chapman & Hall/CRC Cryptography and Series, 2009.
6. Abijit Das, *Computational Number theory*, CRC Press, 2013.
7. Alko R. Meijer, *Algebra for cryptologists*, Springer, 2016.

18CY601 CONCEPTS IN SYSTEM SECURITY 3-0-0-3

Program vs processes, Transaction recovery and concurrency control in database systems. Access control mechanisms in general computing systems - Lampson's access control matrix. Mandatory access control, Authentication mechanisms in databases, DAC, MAC, RBAC, SELinux. Auditing in databases, Statistical inferencing in databases, Private information retrieval viewed as a database access problem. Privacy in data publishing, Virtual Private Databases, Hadoop security. Security and protection in operating systems - access control, auditing, trusted computing base with reference to Multics and the commercial Operating Systems such as UNIX/Linux, Mac OS X v10.x and Windows 10. Malware analysis and protection-viruses, worms and Trojans, Rootkits, Ransomware, Polymorphic malware, Malware capture and analysis using honeypots. Execution of data as code ("code Injection"), ASLR, ROP. Common vulnerabilities and Exposures, Secure system configuration, Minimal footprint, Security of booting, Trusted computing, Virtualization techniques for security, Mobile Operating Systems security especially in Android and iOS.

TEXT BOOKS/REFERENCES:

1. Charles P. Pfleeger and Shari Lawrence Pfleeger, *Security in computing*, Prentice Hall Professional Technical Reference, 4th Edition, 2006.
2. M. Gertz and S. Jajodia, *Handbook of Database Security-Applications and Trends*, Springer, 2008.
3. T. Jaeger, *Operating System Security*, Vol. 1 of Synthesis Lectures on Information Security, Privacy and Trust, Morgan & Claypool Publishers, 2008.
4. W. Mauerer, *Professional Linux Kernel Architecture*, John Wiley and Sons, New York, 2008.
5. R Anderson, *Security engineering*, John Wiley & Sons, 2008.
6. Matt Bishop, *Computer security: Art and Science*, Vol. 2, Addison-Wesley, 2012.

18CY602 CRYPTOGRAPHY 3-0-2-4

Stream ciphers: Pseudo-random generators, Attacks on the one time pad, Linear generators, Cryptanalysis of linear congruential generators, The subset sum generator, Case study: *cryptanalysis of the DVD encryption system*. Block ciphers: Pseudorandom functions and permutations (PRFs and PRPs), PRP

under chosen plaintext attack and chosen ciphertext attack, Case study: *DES, AES, modes of operation*. Message integrity: Cryptographic hash functions, message authentication code, CBC MAC and its security, Cryptographic hash functions based MACs, Case study: *SHA512, SHA3, Merkle trees*. Authenticated Encryption-Authenticated encryption ciphers from generic composition, Public key encryption: RSA, Rabin, Knapsack cryptosystems, Diffie-Hellman key exchange protocol, ElGamal encryption, Elliptic curve cryptography. Digital signatures: Generic signature schemes, RSA, ElGamal and Rabin's signature schemes, blind signatures, threshold signature schemes, ECDSA, Signcryption.

TEXT BOOKS/REFERENCES:

1. A. J. Menezes, P. C. V. Oorschot and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1996.
2. O. Goldreich, *Foundations of Cryptography:* Vol. 1, *Basic Tools*, Cambridge University Press, 2001.
3. O. Goldreich, *Foundations of Cryptography:* Vol. 2, *Basic Applications*, Cambridge University Press, 2004.
4. J. Katz and Y. Lindell, *Introduction to Modern Cryptography*, Chapman & Hall/CRC, 2007.
5. Abhijit Das and Veni Madhavan C. E., *Public-Key Cryptography: Theory and Practice*, Pearson Education India, 2009.
6. Abijit Das, *Computational Number theory*, CRC Press, 2013.
7. Dan Boneh and Victor Shoup, *A Graduate Course in Applied Cryptography*,V4, 2017

18CY603 SECURE CODING 2-0-2-3

Security Concepts - Estimating the threats - Common String Manipulation Errors and Vulnerabilities - Stack overflow, Heap overflow, Off-by-one vulnerabilities - Integer Vulnerabilities - Memory management errors - Format string vulnerabilities - Concurrency and File I/O - Race conditions - Rules and recommendations of SEI CERT C coding Standards. Security Development Lifecycle - Security Requirements Engineering, Use/Misuse case - Design - Secure Software Development Principles, Threat Modeling – Implementation. Web Application Development and Security - OWASP Top 10 flaws - Web, Mobile - Cross Site Scripting (XSS), Injection flaws, CSRF, Clickjacking - Mitigation Techniques - Web application hacker's methodology. Compiler Security features, Abstract syntax trees (AST), Program Analysis-Static, Dynamic, Taint Analysis, Program Slicing. Secure Testing Methodologies - Attacking Dependencies, Attacking through the User Interface, Attacking Design, Attacking Implementation.

TEXTBOOKS / REFERENCES:

1. Dafydd Stuttard, and Marcus Pinto, *The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws*, 2nd Edition, John Wiley & Sons, 2011.
2. Robert C. Seacord, *Secure Coding in C and C++*, 2nd Edition, Addison-Wesley Professional, 2013.
3. Robert C. Seacord, *The CERT C Coding Standard: 98 Rules for Developing Safe, Reliable, and Secure Systems*, 2nd Edition, Pearson Education, 2016.
4. Wenliang Du, *Computer Security – A hands-on Approach*, First Edition, Createspace Independent Pub, 2017
5. https://www.owasp.org

18CY621 INTERNET PROTOCOLS 3-0-0-3

Application Layer: Principles of network applications, Web and HTTP/1.1 and HTTP2, FTP, Electronic mail, SMTP, POP3, IMAP, DNS, VoIP, SIP, Socket programming with UDP and TCP. Transport Layer:

Principles behind transport layer services - Multiplexing, Demultiplexing, Reliable data transfer, Flow control, Congestion control. Internet transport layer protocols: UDP – Connectionless transport, TCP – Connection-oriented reliable transport, TCP congestion control. Network Layer: Virtual circuit and datagram networks, IP- Internet Protocol, Datagram format IPv4 addressing, ICMP, IPv6 addressing. Routing algorithms: Link state, Distance vector, Hierarchical routing. Routing in the Internet: RIP, OSPF, BGP, Broadcast and multicast routing. Data Link Layer: Error detection, Correction, Multiple access protocols. LANs: addressing, ARP, Ethernet, Switches, VLANs. Network Management: SNMP Protocol operations and Transport mappings, MIB, ASN, Network experimentation and performance analysis.

TEXTBOOKS / REFERENCES:

1. J. F. Kurose and K. W. Ross, *Computer Networking: A Top-Down Approach*, Pearson Publication, 7th Edition, 2017.
2. L. Peterson and B. Davie, *Computer Networks: A Systems Approach*, 5th Edition, Elsevier Inc., 2011.
3. W. R. Stevens, *TCP/IP Illustrated, Vol.1: The Protocols,* Addison-Wesley, 1994.

18CY622 CYBER FORENSICS 2-0-2-3

Framework for digital forensic evidence collection and processing, Fundamentals of host forensics for Microsoft windows - Kernel and device driver architecture, Registry, Auditing and security architecture. File system handling - Reconstruction of files and directory structures on the FAT and NTFS. Fundamentals of host forensics for Unix derivatives - Linux operating system, Kernel and device drives architecture, Security and audit mechanisms, File system and pseudo file systems, Reconstruction of file and directory structures using UFS and EXT2/3/4 file systems as exemplars. Forensic analysis of database systems, Database tampering, Forensic analysis of database components, Table storage, Transaction logs, indexes, Forensic recovery for table storage. Network device forensics, Investigating logs, Network traffic and web attacks, Mobile device, Social media and wireless forensics, Anti-forensics, Steganography and image file forensics, Email investigation, Social media forensics, Investigating copiers, IVR, Video surveillance, RFID, Sim cards. Cyber laws in India, Case studies and tools.

TEXT BOOKS/REFERENCES:

1. Brian Carrier, *File System Forensic Analysis*, Pearson, 2006.
2. E. Casey, *Handbook of Digital Forensics and Investigation*, Academic Press, 2010.
3. Marjie T. Britz, *Computer Forensics and Cyber Crime*, Pearson, 2012.
4. David Cowen, *Computer Forensics: A Beginners Guide*, Mc Graw Hill Education, 2013.
5. Bill Nelson, Amelia Phillips, Christopher Steuart, *Guide to Computer Forensics and Investigations*, 4th Edition, 2014.

18CY623 APPLIED CRYPTOGRAPHY 3-0-0-3

Protocols for identification and login: Interactive protocols, ID protocols, Password protocols, Challenge-response protocols, Schnorr's identification protocol, Proving properties in zero-knowledge. Authenticated Key Exchange: encryption-based protocol and its attacks, Perfect forward secrecy, Protocol based on ephemeral encryption, Attacks on Insecure variations, Identity protection, One-sided authenticated key exchange, Deniability, Channel bindings, Formal definitions, Security of protocol AKE1, Password authenticated key exchange - Phishing attacks, Protocol PAKE0, Protocol PAKE1, Protocol PAKE2, Explicit key confirmation. Key exchange protocol with an online TTP, Insecure variations of protocol Online TTP, Conference Key Protocols, Key Broadcasting Protocols.

TEXT BOOKS/REFERENCES:

1. A. J. Menezes, P. C. V. Oorschot and S. A. Vanstone, *Handbook of Applied Cryptography* , CRC Press, 1996.
2. J. Pieprzyk, T. Hardjono and J. Seberry, *Fundamentals of computer security* , Springer, 2003.
3. Abhijit Das and Veni Madhavan C. E., *Public-key Cryptography, Theory and Practice* , Pearson Education, 2009.
4. C. Boyd and A. Mathuria, *Protocols for Authentication and Key Establishment,* Springer, 2010.
5. L. Dong and K. Chen, *Cryptographic Protocol: Security Analysis Based on Trusted Freshness*, Springer, 2012.

18CY624 NETWORK SECURITY 2-0-2-3

Techniques for Network Intrusion Detection System: Snort, Signature-based and Anomaly-based detection; Firewalls: packet filters and stateful firewalls, application-aware firewalls, Proxies, NAT, VPN, Honeypots and Honeynets. Single Sign On (SSO), Email encryption: PGP, STARTTLS; IPSec, SSL3.0, TLS 1.2, Attacks on SSL/TLS: Drown attack, Poodle attack, and Secure HTTP, DNSSEC. ARP Cache poisoning, MAC flooding, Port Stealing, DHCP attacks, DNS based attacks, VLAN hopping, Man in the middle attacks. Web Application Security: Security threats, XSS, CSRF, SQL Injection attacks, RFI, DoS/DDoS

TEXT BOOKS/REFERENCES:

1. William Stallings, *Cryptography and Network Security: Principles and Practice*, 7th Edition, Pearson edition, 2016
2. W. Stallings, *Network Security Essentials: Applications and Standards*, 5th Edition, Pearson Prentice Hall, 2013.
3. Bryan Sullivan and Vincent Liu, *Web Application Security, A Beginner's Guide*, McGraw-Hill Education, 2012
4. Behrouz A. Forouzan, *Cryptography & Network Security*, McGraw-Hill, 2007
5. C. Kaufman, R. Perlman and M. Speciner, *Network Security: Private Communication in a Public World*, 2nd Edition, Prentice Hall PTR, 2002.

18CY625 CYBER SECURITY LAB 0-0-6-3

Objectives

1. To configure virtual networks using network simulator
2. To install and exploit security tools for protecting a network
3. To implement cryptographic algorithm for building a secure communication network
4. To exploit the vulnerabilities in a LAN environment to launch attacks
5. To identify and secure network systems from malicious software
6. To identify and exploit vulnerable virtual machine image
7. To perform vulnerability assessment of wireless devices and audit the same with penetration testing
8. To analyze the source code and carry out a reverse engineering of binaries and executables
9. To apply machine learning algorithms in intrusion detection dataset
10. To create, install, update, and disassemble Android applications.

The experiments make use of Kali Linux distro and other open source security tools. Latest version of these tools and distros are available in the Cyber Security Lab.

Experiment No. 1: LAN based Network Security

Set up a simple LAN as shown in Figure 1. M1-3 and S1-3 are machine which have Linux and Windows running.

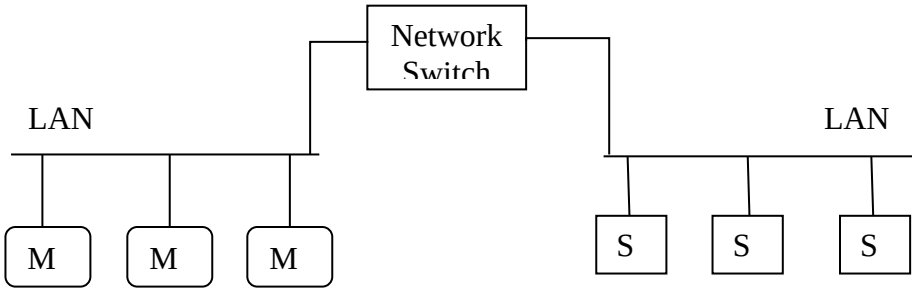

Figure 1: A Simple LAN environment

1. Configure LAN-1 and LAN-2 as separate VLANs in the Network Switch.
   - Use inter VLAN ACL
2. Create a SPAN port in the Network switch and send the mirrored traffic to a promiscuous mode port for the purpose of IDS and other packet analysis. Practice port based and VLAN based mirroring.
3. Familiarize with 802.1x, Network Admission Control, Microsoft NAP, RADIUS protocol, RADIUS per port ACL

Experiment No. 2: Network reconnaissance and Protection

- Installing 'iptable' in Ubuntu VM to allow/block communication between VMs
  - Installing Email server and Web server in VMs. Usage of Firewall (iptable) in blocking/allowing a sub-network from accessing the servers
  - Configuring iptable to block Telnet inbound and outbound connections

1. Use 'nmap' tool to perform vertical and horizontal scanning for checking open and closed ports. Use nmap commands for performing the following experiments:
   - Use ping sweeping to determine which hosts are running
   - Check for vulnerable services available using TCP connect scans
   - Perform OS Fingerprinting to determine the OS of target machine
   - Choose different options under each category according to your creativity.
   -

Experiment No. 3: Application of Cryptographic algorithms using Crypto Tools.

Establish a Client-Client Secure communication protocol as shown in Figure 2.

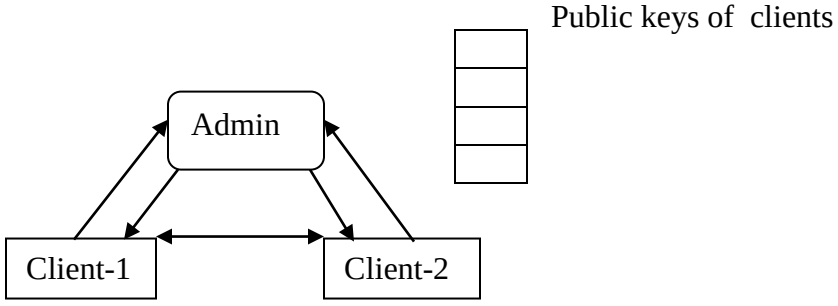

Figure 2: Secure Communication

The Client machines (Client-1 and Client-2) and Admin machine are installed in different VMs. All the three machines are interconnected through a network switch with different IP addresses. The Admin runs a program that generates 2048 bit RSA public and private key for a Client that wants to communicate. Admin generates 2048 bit RSA public and private key for Client-1 and Client-2. The private keys are distributed to client machines and public keys are stored in a structure in the admin machine. When Client-1 wants to send message to Client-2, it encrypts the messages with public key of Client-2. The message is decrypted by Client-2 with its private key. Similar communication pattern from Client-2 to Client-1 need to be maintained.

Manually capture the traffic between the hosts to ensure the proper working of the encryption. Construct an asynchronous communication between Client-1 and Client-2. Run a Wireshark/ TCPdump at the SPAN/Promiscuous port of the network switch and identify the communication between the communicating entities (Admin, Client-1, and Client-2).

Experiment No. 4: LAN based insider attacks

Make use of Ettercap/arpspoof tool to perform ARP Cache Poisoning based attacks in a LAN environment:

1. Perform Denial of Service (DoS) attacks using ARP Cache Poisoning attacks
2. Perform DNS Spoofing attack using ARP Cache Poisoning attacks
3. Perform Password stealing (over plaintext) using ARP Cache Poisoning attacks
4. Invoke 'sslstrip tool' for stealing password from any machine that is connected in a LAN by stripping the https connection.

For all the above attacks, observe the ARP cache table, CAM table, etc., before and after the attack. Run Wireshark and observe the traffic patterns before and after the attack.

Experiment No. 5: Malware & Attack evasion Techniques

Install Virtual Machines (VM) – Win2000 Server and Win 8. Install 'Poison Ivy' Remote Administration Toolkit in Server VM (admin.exe). Build and Generate a client.exe (client) program. Install the client.exe program in the Win XP machine. The client.exe communicates with the admin.exe in Win Server2000 VM.

Consider the following tasks:

1) Enlist the processes, installed programs, dump the LM hashes, etc. from the Win XP machine
2) Does 'client.exe' enlisted in the process list? If, write a procedure/program to hide the process (client.exe) from process table list?
3) Set Firewall rules in Windows machine to block communication between the two VMs.

Experiment No. 6: Vulnerability Assessment and Penetration Testing (VAPT) Lab

Perform Vulnerability Assessment and Penetration Testing aimed at virtual machine images of computer network with distributed misconfigurations and vulnerabilities. The virtual machine images contain vulnerable network services, web services, social engineering and buffer overflow to be exploited. Generate VAPT Pen Test report based on standards such as Pen Test Report SANS, Offensive-security, or ISACA.

Experiment No. 7: Wireless Security Lab

Perform a VA/PT on your local Wi-Fi network and try automated attacks with NetStumbler and Kismat to gather information wireless network and try attacks like CowPatty and Airsnort. Further execute aircrack-ng to simulate attacks 802.11 WEP and WPA-PSK keys for auditing wireless networks and performing

airodump, aircrack, airmon, airbase, aireplay and airtun using Kali 2.0 (Sana) Linux. Attempt a Wi-Fi sniffing to gather location data which can be used to identify device parameters of wireless communication devices.

Experiment No. 8: Reverse Engineering Lab

Use Metasploit (open-source exploit framework) to write and test your own exploit into any PC/Site with existing payloads using Virtual Machines in Ubuntu Host and Windows XP Virtual disk. These traces should be executed in OllyDbg step by step, and debug the protocols every single command, laidback with registers and flags, with buffer information. Also debug standalone DLL's like Message Box and wsprintf. Use IDA Pro (evaluate a limited version of the disassembler) to examine a protected and obfuscated sample executable. (.NET Reflector can be used to search through, the class hierarchies of .NET assemblies, even without any source code).
Perform static and dynamic code auditing.

Experiment No. 9: Security Data Analytics Lab

Download KDD CUP'99 dataset (http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html). Separate the datasets into two class dataset such as normal-dos, normal-probe, normal-u2r, and normal-r2l. Any of the toolkits such as R, Weka, RapidMiner, Matlab, etc., can be used.

1. Apply Correlation based Feature Selection Algorithms (FSA) in order to derive the subset of features that represent the dataset. What is the gain in applying FSA? Is there any change in detection rate with and without applying FSA? How the execution time/model building time varies with and without applying FSA?
2. Apply Multilayer Perceptron Classification algorithm and calculate the metrics such as detection rate, false alarm rate, ROC value, F-measure for each class. Also, vary the parameters such as momentum and learning rate and calculate the metrics.
3. Apply Simple *k*-Means Clustering algorithm and calculate the metrics such as detection rate, false alarm rate, ROC value, F-measure for each class. Also, vary the parameters such as Euclidean and Manhattan distances and calculate the metrics.
4. Apply RIPPER algorithm (rule based classifier) to formulate the rules extracted from the dataset. Determine the number of rules extracted and enumerate each rule.

Devise a procedure/mechanism in building a dataset for the following:

1. Network Intrusion Detection system dataset
2. Host Intrusion Detection system dataset
3. Malware dataset
4. Botnet dataset
5. Spam email, Web browsing, Net flow data, firewall logs, Anomilize Tools, DNS records
   Refer: http://www.unb.ca/research/iscx/dataset/index.html

Systematically generate the dataset involving each of the four identified modules – Experimental set up, Data collection, Feature construction and Class labeling.

Experiment No. 10: Mobile & Smart Phone Security Lab

Familiarize with mobile .apk files. Create your own Android app. Find vulnerable app in play store and perform forensics analysis on the app and document the inferences.

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

18CY701 DATA MINING AND MACHINE LEARNING IN CYBER SECURITY 2-0-2-3

Introduction to Data Mining and Machine Learning, Review of Cyber security Solutions – Signature, Anomaly and Hybrid detection, Classical Machine learning paradigms for Data Mining, Fundamentals of Supervised and Unsupervised Machine Learning algorithms, Improvements on Machine learning methods, Challenges in Data Mining and Machine learning. Supervised learning for Misuse/signature detection, Machine learning for anomaly detection using Probabilistic Learning, Unsupervised learning, Combination learners, Evaluation methods, Hybrid detection. Machine learning for scan detection and

Network traffic profiling, Privacy-Preserving Data Mining, Feature Selection – Methods and steps. Deep Learning - Deep Feedforward Networks, Convolution Networks, Sequence Modeling - Recurrent and Recursive Nets, Representation Learning, Structured Probabilistic Models for Deep Learning, Deep Generative Models - Applications of deep learning in malware analysis and information retrieval.

TEXT BOOKS/REFERENCES:

1. Tom M Mitchell, *Machine Learning*, McGraw Hill, 1997.
2. Jiawei Han, Micheline Kamber, Jian Pei, *Data Mining: Concepts and Techniques*, 3rd edition, 2011.
3. D. K. Bhattacharyya and J. K. Kalita, *Network Anomaly Detection: A Machine Learning Perspective*, 1st Edition, Chapman and Hall/CRC, 2013.
4. T. Dunning and E. Friedman, *Practical Machine Learning - A New Look at Anomaly Detection*, O'Reilly, 1st edition, 2014.
5. Ian Goodfellow, Yoshua Bengio, Aaron Courville, *Deep Learning*, MIT Press, 2016.

18CY702 DISTRIBUTED AND CLOUD COMPUTING 2-0-2-3

Spatial and temporal distribution of processes. Message passing, Synchronization, Mutual exclusion. Communicating Sequential Processes (CSP). Distributed Tuple Space and Linda. Clients and servers, RPC, RMI. Scalability up and out, Elasticity, Data centers, Cloud Models, MapReduce/ Hadoop, SPARK, Key-value stores, Security and Privacy, Amazon AWS, Google App Engine, Microsoft Azure, OpenStack, Docker.

TEXT BOOKS/REFERENCES:

1. M. Ben-Ari, *Principles of Concurrent and Distributed Programming*, Addison- Wesley/Pearson, 2nd Edition, 2006.
2. George Coulouris, Jean Dollimore, Tim Kindberg, and Gordon Blair, *Distributed Systems: Concepts and Design*, 5th Edition, 2011.
3. Thomas Erl, Ricardo Puttini, and Zaigham Mahmood, *Cloud Computing: Concepts, Technology and Architecture*, Prentice Hall, 2013
4. Scala + Akka Documentation, http://doc.akka.io/docs/akka/current/scala.html
5. Java tutorial, http://download.oracle.com/javase/tutorial/

18CY703 DESIGN AND ANALYSIS OF ALGORITHMS 2-0-2-3

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

TEXT BOOKS/REFERENCES:

1. R. Motwani and P. Raghavan, *Randomized Algorithms*, Cambridge University Press, 1995.

2. D. E. Knuth, *Art of Computer Programming*, Vol. 3, *Sorting and Searching*, 2nd Edition, Addison-Wesley Professional, 1998.
3. T. Cormen, C. Leiserson, R. Rivest and C. Stein, *Introduction to Algorithms*, 3rd Edition, McGraw-Hill, 2009.
4. J. J. McConnell, *Analysis of Algorithms: An Active Learning Approach*, Jones & Bartlett Publishers, 2001.
5. S. Dasgupta, C. H. Papadimitriou and U. V. Vazirani, *Algorithms*, McGraw-Hill, 2008.

18CY704 WIRELESS NETWORKING AND SECURITY 2-0-2-3

Overview of Electromagnetic Theory and Propagation, Digital Modulation techniques, Signal Encoding Techniques, Spread Spectrum Techniques, Multiple Access, IEEE 802 standards. Cellular Concept, Standards, GSM Architecture, Handoff & Roaming, Interference, CDMA, 3G and 4G Systems, Satellite Networks & GPS, Wi-Max, Ultra Wide Band, IEEE 802.11 Standards, Bluetooth and other IEEE 802.15 standards. Threats to Wireless networks, Attacks on 802.11 networks – WEP, WPA, Wireless clients, Attacks on Bluetooth network, Eavesdropping, Privacy Challenges, Risks – Denial of Service, Insertion Attacks, Surveillance, War Driving, Jamming and Denial of Service. Authentication, Encryption/Decryption in GSMs. Securing the WLAN, WEP, RC4, WPA/ WPA2, IEEE 802.11i, Security in Bluetooth, Wi-MAX, UWB and Satellite networks, Android Security, 5G and security.

TEXT BOOKS/REFERENCES:

1. Joshua Wright and Johnny Cache, *Hacking Exposed Wireless*, 3rd Edition: Wireless Security Secrets & Solutions, McGraw-Hill Education, 2015.
2. Jon Edney and William A. Arbaugh, *Real 802.11 Security: Wi-Fi Protected Access and 802.11i*, Addison-Wesley Professional,1st Edition, 2003.
3. H. Chaouchi and Maryline Laurent-Maknavicius, *Wireless and Mobile Networks Security*, Wiley, 2009.
4. K. Pahlavan and P. Krishnamurthy, *Principles of Wireless Networks: A Unified Approach*, Prentice Hall, 2002.
5. C. Peikari and S. Fogie, *Maximum Wireless Security*, Sams Publishing, 2002.
6. W. Stallings, *Wireless Communications and Networks*, 2nd Edition, Pearson Education Ltd, 2009.

18CY705 CODING AND INFORMATION THEORY 2-0-2-3

Information theory- Information, Entropy, Discrete memoryless source, Source coding - Shannon-Fano coding, Huffman coding, Lempel-Ziv and arithmetic codes, Rate distortion theory, Optimum Quantizer Design. Discrete memoryless channel, Mutual information, Channel capacity, Shannon limit, Error control codes - Linear block codes, Error detection and correction, Hamming codes, Reed Muller codes, Golay codes, Cyclic codes, Binary BCH codes, Reed Solomon codes, Decoding algorithms, Trellis representation of codes, Convolution codes and its applications, Viterbi algorithm and decoding.

TEXT BOOKS/REFERENCES:

1. R. E. Blahut, *Algebraic Codes for Data Transmission*, Cambridge University Press Cambridge, UK, 2003
2. S. Lin and D.J. Costello, *Error Control Coding - Fundamentals and Applications*, 2nd Edition, Pearson Education Inc., NJ., USA, 2004.
3. Elwyn R. Berlekamp, *Algebraic Coding Theory*: *Revised Edition*, World Scientific, 2015.

4. Thomas M. Cover, and Joy A. Thomas, *Elements of information theory*, John Wiley & Sons, 2012.

18CY706 CRYPTOGRAPHIC HARDWARE AND EMBEDDED SYSTEMS 2-0-2-3

Introduction to Verilog- Structure, Constructs, and Conventions. Modeling at Gate level, Data flow level, Behavior level, and switch level. Design, Simulation, and Synthesis of digital circuits, Modules, and Systems. Functions, Tasks, User defined primitives, Compiler directives. Queues, PLAs, and FSMs. FPGAs – blocks inside, their features and use. IDE and its use, FPGA based design realizations, Design of finite field arithmetic operations, Representative designs with AES, ECC and Hash Algorithms.

TEXT BOOKS/REFERENCES:

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

18CY707 STEGANOGRAPHY AND OBFUSCATION 2-0-2-3

Steganographic security, Data hiding in raw images, Spatial and transform domain steganography, JPEG format, S-tool, J-Steg, OutGuess. Steganalysis, Case study*: Data hiding in digital Audio and Video, Operating System Data Hiding, Virtual Data Hiding, Data Hiding in Network Protocols, Data Hiding among Android Mobile Devices and Apple iOS, Forensics and Anti-Forensics, Mitigation Strategies*. Obfuscation - Methods of attack and defense, Program analysis, Code obfuscation- Complicating control flow, Opaque predicates, Data encoding, Applications of Code Obfuscation. Software Watermarking, Models of watermarking, Modeling Watermark Detection by Correlation. Visual Cryptography, Attacks and benchmarks for data hiding systems.

TEXTBOOKS/ REFERENCES:

1. I. J. Cox, M. L. Miller, J. A. Bloom , J. Fridrich and T.Kalker, *Digital Watermarking and Steganography*, 2nd Edition, The Morgan Kaufmann Series in Multimedia Information and Systems, 2002.
2. J. Fridrich, *Steganography in Digital Media: Principles, Algorithms, and Applications*, 1st Edition, Cambridge University Press, 2010.
3. C. Collberg and J. Nagra, *Surreptitious Software: Obfuscation, Watermarking, and Tamperproofing for Software Protection*, Addison-Wesley, 2010.
4. M. T. Raggo and C. Hosmer, *Data Hiding: Exposing Concealed Data in Multimedia, Operating Systems, Mobile Devices and Network Protocols*, 1st Edition, Syngress, 2012.

18CY708 FORMAL METHODS FOR SECURITY 2-0-2-3

Formal Methods – Propositional and Predicate logic, and theorem-proving, Fixed-points and their role in program analysis and model-checking, Verification of sequential programs using weakest preconditions and inductive methods, and verification of concurrent and reactive programs/systems using model-checking and propositional temporal logic (CTL and LTL), Application of static and dynamic program

analysis and model-checking for detecting common security vulnerabilities in programs and communication protocols, Information flow and taint analysis for security of web applications, pi-calculus for formal modelling of mobile systems and their security. SPIN, PVS, TAMARIN, Frama-C and Isabelle tools.

TEXT BOOKS/REFERENCES:

1. Edmund M. Clarke, Orna Grumberg and Doron Peled, *Model Checking*, MIT Press, 1999.
2. Lloyd, J.W., *Logic and Learning: Knowledge Representation, Computation and Learning in Higher-order Logic*, Springer Berlin Heidelberg, 2003.
3. M. Ruth and M. Ryan, *Logic in Computer Science - Modelling and Reasoning about Systems*, Cambridge University Press, 2004 .
4. G. Bella, *Formal Correctness of Security Protocols*, Springer, 2009.
5. Datta A, Jha S, Li N, Melski D and Reps T, *Analysis Techniques for Information Security*, Synthesis Lectures on Information Security, Privacy, and Trust, 2010.

18CY709 ANDROID SECURITY 2-0-2-3

App Development, Refresher Linux OS, Emulator and ADB, APK Internals, Networking, Device Rooting, Refresher TCP/IP Attacks, TCP/IP Attacks Using Android, DAC and MAC Permissions, Android Internals, Framework, Init, Zygote, Binder, Service Manager, Activity Manager, Reverse Engineering, Malware Analysis, Bouncer, Code Injection, Privacy Violation, System Call Hardening, ASLR, ROP, Framework Exploits.

TEXT BOOKS/REFERENCES:

1. Y. Karim, *Embedded Android*, Vol. 1, O'Reilly Media, 2013.
2. E. Nikolay, *Android Security Internals: An In-Depth Guide to Android's Security Architecture*, No Starch Press, 2014.

18CY710 SECURITY IN CLOUD COMPUTING 2-0-2-3

The trade-offs and differences among cloud offerings such as SaaS, PaaS and IaaS, Key-value stores and their trade-offs against transactional SQL stores, Implementations of classic key-value stores such as Big Table & Dynamo, The use of consensus in distributed systems and its implementation in Paxos and Raft, MapReduce and other parallel processing frameworks, Server and network virtualization, Security in the cloud-infrastructure and data, Significant hands-on project experience with a chosen cloud computing framework, Privacy, Side Channel Attack, Insider attack on cloud computing, SAS-70 Certificates HIPAA, Public and Private cloud, Key Management problem for cloud, Homomorphic and Searchable Encryption.

TEXT BOOKS/REFERENCES:

1. S. Ghemawat, H. Gobioff, and S. T. Leung, *The Google file system*, In ACM symposium on operating systems review, Vol. 37, No. 5, pp. 29-43, 2003.
2. J. Dean and S. Ghemawat, *MapReduce: simplified data processing on large clusters*, Commun., ACM 51, no.1, 107-113, 2008.
3. R. Chow, P. Golle, M. Jakobsson, R. Masuoka, Jesus Molina Elaine Shi and Jessica Staddon, *Controlling data in the cloud: outsourcing computation without outsourcing control*, In Proceedings of the ACM workshop on Cloud computing security, pp. 85-90, 2009.

4. T. Mather, S. Kumaraswamy and S. Latif, *Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance,* O'Reilly Series, 2009.
5. T. Erl, R. Puttini and Z. Mahmood, *Cloud Computing: Concepts, Technology & Architecture*, Prentice Hall, 2013.

18CY711 SPECIAL TOPICS IN CRYPTOGRAPHY 2-0-2-3

Lattice based cryptography - Integer lattices, Hard problems on lattices - Shortest vector problem, The SIS problem, The learning with errors (LWE) problem , The ring LWE problem, Trapdoor sampling from a lattice, Signatures from lattice problems, Public-key encryption from lattices, Homomorphic encryption, Elliptic curve cryptography and pairings, BLS signatures, Group signatures, Identity based encryption, Broadcast encryption.

TEXT BOOKS/REFERENCES:

1. Daniele Micciancio and Shafi Goldwasser, *Complexity of Lattice Problems: A Cryptographic Perspective* , 2002.
2. J. H . Silverman, *The Arithmetic of Elliptic Curves*, Vol. 106, Dordrecht: Springer, 2009.
3. C. Boyd and A. Mathuria, *Protocols for Authentication and Key Establishment,* Springer, 2010.
4. L. Dong and K. Chen, *Cryptographic Protocol: Security Analysis Based on Trusted Freshness*, Springer, 2012.
5. Peikert, C., *A decade of lattice cryptography*, Foundations and Trends in Theoretical Computer Science, 10(4), pp.283-424, 2016.
6. Dan Boneh and Victor Shoup, *A Graduate Course in Applied Cryptography*,V4, 2017.
7. *Rings and Integer Lattices in Computer Science*, lectures notes from the Bellairs-McGill workshop on Computational Complexity in 2007.

18CY712 BLOCKCHAIN TECHNOLOGY 2-0-2-3

Blockchain Data structure, Hash chain, Distributed database, Index structure, Blockchain Architecture - Hashes, Transactions, Asymmetric-Key Cryptography, Addresses and Address Derivation, Private Key Storage, Ledgers, Blocks, Chaining Blocks. Consensus and multiparty agreements - Protocols, Proof of Work, Proof of Stake, Delegated Proof of Stake, Proof of Elapsed Time, Deposit based consensus, Proof of importance, Federated consensus or Federated Byzantine consensus, Reputation-based mechanisms, Practical Byzantine Fault Tolerance. Blockchain implementation, Forking - Soft Fork, Hard Forks, Cryptographic Changes and Forks, Smart contract programing, Blockchain Platforms – Cryptocurrencies (Bitcoin, Litecoin, Ethereum, Ripple), Hyperledger, Ethereum. Blockchain - Outside of Currencies, IPFS protocol and Blockchain, Blockchain Concurrency and scalability, Network models and timing assumptions.

TEXT BOOKS/REFERENCES:

1. Abhijit Das and Veni Madhavan C. E., *Public-Key Cryptography: Theory and Practice*, Pearson Education India, 2009.
2. Melanie Swan, *Blockchain - Blueprint for a new economy*, O'Reilly Media, Inc., 2015.
3. A. Narayanan, J. Bonneau, E. Felten, A. Miller, S. Goldfeder, *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*, Princeton University Press, 2016

4. Roger Wattenhofer, CreateSpace, *The Science of the Blockchain*, Independent Publishing Platform, 2016
5. Imran Bashir, *Mastering Blockchain*, 2017.
6. Andreas M. Antonopoulos, *Mastering Bitcoin - Programming the Open Blockchain*, O'Reilly Media, Inc., 2017
7. Alex Leverington, *Ethereum Programming*, Packt Publishing Limited, 2017.
8. Draft NISTIR 8202, Blockchain Technology Overview - NIST CSRC, 2018.

18CY713 SECURE SYSTEMS ENGINEERING 2-0-2-3

Information flow and vulnerability model to build security into life cycle phase of software (and hardware) components, Vulnerability analysis into architecture and design process, Access-controlled and clean environment to build software, Target environment hardening and secure application deployment, Introduction to hardware security – Physical and side channel attacks and its countermeasures, Tamper resistance, Balancing security and usability – User authentication mechanisms, Secure browsing, Social media and data sharing, Countermeasures for possible social engineering attacks in design, Secure interactive design, Privacy issues in Human Computer Interaction, Security Economics: Risk assessment – CVSS scoring and selection of appropriate countermeasures with cost-benefit trade-offs, ISO 27001:2013 – ISMS, Overview of security in cloud computing, Internet of Things (IoT) and Mobile platforms, Recent exploits and attack scenarios.

TEXT BOOKS/REFERENCES:

1. S. Garfinkel and L. F. Cranor, *Security and Usability: Designing Secure Systems That People Can Use*, O'Reilly, 2008.
2. Tim Mather, Subra Kumaraswamy, Shahed, *Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance*, O'Reilly, 2009.
3. Anderson, Ross J., *Security Engineering: A Guide to Building Dependable Distributed Systems*, John Wiley & Sons, 2010.
4. M. Tehranipoor, and C. Wang, *Introduction to Hardware Security and Trust*, Springer, 2011.
5. C. W. Axelrod, *Engineering Safe and Secure Software Systems*, Artech House, 2013.
6. Antonio Borghesi and Barbara Gaudenzi, *Risk Management: How to Assess, Transfer and Communicate Critical Risks*, Springer, 2013.
7. Steve Watkins, *An Introduction to Information Security and ISO27001:2013: A Pocket Guide*, 2nd Edition, IT Governance Publishing, 2013.
8. Shancang Li, Li Da Xu, *Securing the Internet of Things*, 2017.