M. Tech Program in 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
16MA 608	FC	Mathematical Foundations for Cyber Security	4 0 0	4
16CY 602	FC	Concepts in System Security	3 0 0	3
16CY 603	FC	Cryptography	3 0 1	4
16CY 611	SC	Internetworking- Protocols and Security	3 0 0	3
16CY 612	SC	Data Mining and Machine Learning in Cyber Security	3 0 1	4
16HU 601	HU	Cultural Education *		P/F
			Credits	**18**

* Non-Credit Course

Second Semester

Course Code	Type	Course	L T P	Cr
16CY 613	SC	Cyber Forensics	2 0 1	3
16CY 614	SC	Cryptographic Protocols and Standards	3 0 0	3
16CY 604	FC	Secure Coding	3 0 1	4
16CY 615	SC	Cyber Security Lab	0 0 3	3
	E	Elective I	2 0 1	3
	E	Elective II	2 0 1	3
16 EN 600		Technical Writing*		P/F
			Credits	**19**

* Non-Credit Course

Third Semester

Course Code	Type	Course	L T P	Cr
	E	Elective III	3 0 1	4
	E	Elective IV	2 0 1	3
16CY 798	P	Dissertation		10
			Credits	**17**

Fourth Semester

Course Code	Type	Course	L T P	Cr
16CY 799	P	Dissertation		12
			Credits	**12**

Total Credits: 66

List of Courses

Foundation Core

Course Code	Course	L T P	Cr
16MA 608	Mathematical Foundations for Cyber Security	4 0 0	4
16CY 602	Concepts in System Security	3 0 0	3
16CY 603	Cryptography	3 0 1	4
16CY 604	Secure Coding	3 0 1	4

Subject Core

Course Code	Course	L T P	Cr
16CY 611	Internetworking - Protocols and Security	3 0 0	3
16CY 612	Data Mining and Machine Learning in Cyber Security	3 0 1	4
16CY 613	Cyber Forensics	2 0 1	3
16CY 614	Cryptographic Protocols and Standards	3 0 0	3
16CY 615	Cyber Security Lab	0 0 3	3

Electives

Course Code	Course	L T P	Cr
	Elective I		
16CY 701	Mobile & Wireless Networking and Security	2 0 1	3
16CY 702	Language-Based Security	2 0 1	3
16CY 703	Network Security	2 0 1	3
	Elective II		
16CY 704	Steganography and Obfuscation	2 0 1	3
16CY 705	Information Security and Risk Management	3 0 0	3
16CY 706	HDL and Cryptographic Applications	2 0 1	3
	Elective III		
16CY 707	Coding and Information Theory	3 0 1	4
16CY 708	Security in Cloud Computing	3 0 1	4
16CY 709	Design and Analysis of Algorithms	3 0 1	4
	Elective IV		
16CY 710	Formal Methods for Security	2 0 1	3
16CY 711	Secure Systems Engineering	2 0 1	3
16CY 712	Security in Internet of Things	2 0 1	3
16CY 713	Android Security	2 0 1	3

Project

Course Code	Courses	L T P	Cr
16CY 798	Dissertation		10
16CY 799	Dissertation		12

16MA 608 MATHEMATICAL FOUNDATIONS FOR CYBER SECURITY 4-0-0-4

Elementary Number Theory – Divisibility, Prime numbers; Algorithms for primality testing and Integer Factorisation; Arithmetic functions, Congruence, Quadratic Residues, Primitive roots. Algebraic Structures - Groups, Rings and Fields; Polynomials over Finite Field - Order of Polynomials, Primitive polynomials. Extension Fields. Algorithms for Discrete Logarithm, Arithmetic of Elliptic Curves, Bilinear maps, Solving nonlinear system of equations - XL algorithm and Grobner basis techniques. Discrete and Continuous random variables, Expectation and Variance, Binomial, Poisson and Normal distributions, Cumulative distribution function, Joint probability distribution of functions of random variables, Expectations of sums of random variables, Covariance and variance of sums, Bayes' theorem.

TEXT BOOKS/REFERENCES:

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

16CY 602 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. Matt Bishop, *Computer Security: Art and Science*, Vol. 200, Addison-Wesley, 2012.
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. Charles P. Pfleeger and Shari Lawrence Pfleeger, *Security in Computing, Fourth Edition,* Prentice Hall Professional Technical Reference, 2006.
6. R Anderson, *Security Engineering*, John Wiley & Sons, 2008.

16CY 603 CRYPTOGRAPHY 3-0-1-4

Shannon ciphers and perfect security, Computational ciphers and semantic security, Pseudo-random generators, Stream Ciphers: One time pad, Composing PRGs, Pseudorandom bit generators & Pseudorandom functions: provably secure pseudorandom generators, existence of pseudorandom generators. Pseudorandom functions and permutations (PRFs and PRPs), PRP under chosen plaintext attack and chosen ciphertext attack, usage of PRFs and PRPs in shared random function model and in modeling block ciphers. Construction of PRF, applications of PRFs: cryptographically strong hashing, private-key encryption. Symmetric encryption schemes: Block ciphers and modes of operation, indistinguishability under chosen plaintext and chosen ciphertext attack. One way and trapdoor functions, Discrete Logarithm functions, RSA functions. Publickey encryption: RSA, Rabin, Knapsack cryptosystems and ECC; polynomial indistinguishability, semantic security; probabilistic public key encryption. Message authentication & Digital signatures: designing MACs using PRFs, CBC MAC and its security, universal hash based MACs, MACing with Cryptographic hash functions, Authenticated encryption; trapdoor function model, Generic signature schemes, RSA, ElGamal and Rabin's signature schemes, probabilistic signatures, signature scheme based on Claw-free trapdoor permutations, blind signatures, threshold signature schemes.

TEXT BOOKS/REFERENCES:

1. A. J. Menezes, P. C. V. Oorschot and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1996.
2. O. Goldreich, *Foundations of Cryptography:* Vol. 1, 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. J. H . Silverman, *The Arithmetic of Elliptic Curves*, Vol. 106, Dordrecht: Springer, 2009.
6. Abhijit Das and Veni Madhavan C. E., *Public-Key Cryptography: Theory and Practice: Theory and Practice*, Pearson Education India, 2009.
7. Abijit Das, *Computational Number theory*, CRC Press, 2013.

16CY 604 SECURE CODING 3-0-1-4

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 and CERT Java coding Standards. Recommended Practices - Security Development Lifecycle - Security Requirements Engineering, Use/Misuse case - Design - Secure Software Development Principles, Threat Modeling - Implementation - Compiler Security features, abstract syntax

trees (AST), static analysis, Software Assurance and Testing- Software Assurance overview, Testing threat categories, Assessing Risk, Secure Testing Methodologies - Attacking Dependencies, Attacking through the User Interface, Attacking Design, Attacking Implementation. Web Application Security - OWASP Top 10 flaws - Cross Site Scripting (XSS), Injection flaws, CSRF, Clickjacking - Mitigation Techniques - Web application hacker's methodology.

TEXTBOOKS / REFERENCES:

1. Robert C. Seaford, *Secure Coding in C and C++*, Addison-Wesley Professional, 2005.
2. Robert C. Seacord, *The CERT C Coding Standard: 98 Rules for Developing Safe, Reliable, and Secure Systems.* Pearson Education, 2014.
3. Dafydd Stuttard, and Marcus Pinto, *The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws*, Second Edition, John Wiley & Sons, 2011.
4. https://www.securecoding.cert.org/confluence/display/seccode/SEI+CERT+Coding+Standards.
5. https://www.owasp.org/index.php/Top10#OWASP_Top_10_for_2013.

16CY 611 INTERNETWORKING - PROTOCOLS AND SECURITY 3-0-0-3

Network services and applications: HTTP, SMTP, FTP, DNS, peer-to-peer systems, Transport architectures, TCP, UDP, ICMP, TCP congestion control, Routing and forwarding, intra-domain and inter-domain routing algorithms, Internet Protocol, IPV6, Link layers and local area networks: Ethernet, Multimedia communications and quality of service, Network measurement, inference, and management, Network experimentation and performance analysis. Security: ARP attacks and ARP poisoning, DNS attacks, SYN flood attacks and its mitigation, UDP ping-pong and fraggle attacks, TCP port scanning and reflection attacks.

TEXT BOOKS/REFERENCES:

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

16CY 612 DATA MINING & MACHINE LEARNING IN CYBER SECURITY 3-0-1-4

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, Soft computing, 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. T. Dunning and E. Friedman, *Practical Machine Learning - A New Look at Anomaly Detection*, First Edition, O'Reilly, 2014.
2. D. K. Bhattacharyya and J. K. Kalita, *Network Anomaly Detection: A Machine Learning Perspective*, First Edition, Chapman and Hall/CRC, 2013.
3. S. Dua and X. Du, *Data Mining and Machine Learning in Cybersecurity*, First Edition, Auerbach Publications, 2011.
4. L. Deng and D. Yu, *Deep learning: Methods and applications*, Foundations and Trends in Signal Processing, Vol. 7, Issue 3–4, pp. 197-387, 2014.

16CY 613 **CYBER FORENSICS** **2-0-1-3**

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

TEXT BOOKS/REFERENCES:

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

16CY 614 **CRYPTOGRAPHIC PROTOCOLS AND STANDARDS 3-0-0-3**

Goals for authentication and Key Establishment, Formal Verification of Protocols, Complexity Theoretic Proofs of Security. Protocols Using Shared Key Cryptography – Entity Authentication Protocols, Server-Less Key Establishment, Server-Based Key Establishment, Zero Knowledge interactive proofs. Authentication and Key Transport using Public Key Cryptography – Design Principles for Public Key Protocols, Entity Authentication Protocol, Key Transport Protocols. Key Agreement Protocols, Key Control, Unknown Key Share Attacks, Classes of Key Agreement- Diffie Hellman Key Agreement, MTI Protocols, Diffie Hellman-Based Protocols. Protocols not based on Diffie Hellman. Conference Key Protocols – Generalizing Diffie Hellman Key Agreement. Conference Key Agreement Protocols- Identity Based Conference Key Protocols, Conference Key Agreement without Diffie Hellman, Conference Key Transport Protocols. Key Broadcasting Protocols, Secret Sharing based Protocols. Pairing based cryptographic protocol- ID based encryption schemes, Boneh and Franklin's Scheme, Shamir's encryption and signature schemes, Okamoto's scheme, Gunther's scheme, Girault's scheme. Homomorphic encryption. Cryptographic standards: International standards, Banking security standards, International security architectures and frameworks, U.S. government standards (FIPS), Internet standards and RFCs, Ordering and acquiring standards.

TEXT BOOKS/REFERENCES:

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

16CY 615 **CYBER SECURITY LAB 0-0-3-3**

1. Installing and exploiting security tools for protecting a network.
2. Implementation of cryptographic algorithm for building a secure communication network.
3. Analysis of malicious software in tampering with the operating system process list.
4. Exploiting the vulnerabilities in a LAN environment to launch attacks.
5. Usage of forensics tools in gathering information from communication devices and host machines.
6. Identifying and securing the systems from malicious software.
7. Performing a vulnerability assessment of Wireless devices and audit the same with penetration testing.
8. Analyze the source code and carry out a reverse engineering of binaries and executables.

9. Application of machine learning algorithms in intrusion detection dataset
10. Create, install, update, and disassemble android applications.

Some of the experiments makes use of Kali Linux distro & Metaspolit Framework 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.

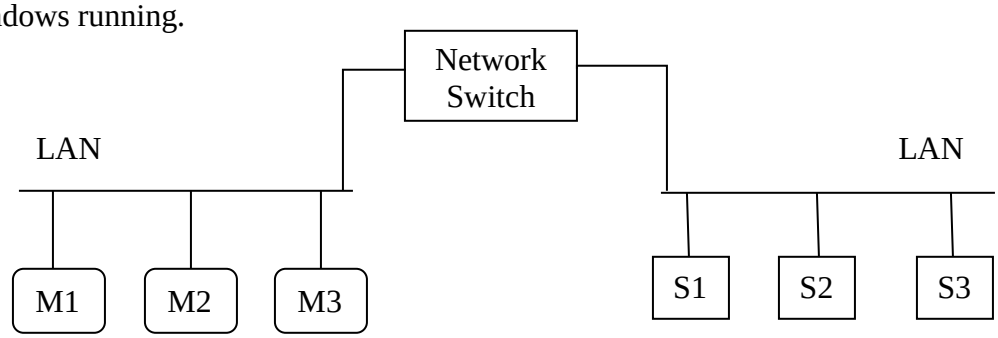

Figure 1: A Simple LAN environment

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
2. 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.
3. Invoke 'p0f' Passive OS Fingerprinting tool to perform the following
   - Operating system and service pack
   - Installed applications
   - Open ports available and services running in the machine

Experiment No. 3: Secure communication between hosts using, SSL-TLS, IPSec, and Secure Layer 2 VPNs.

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

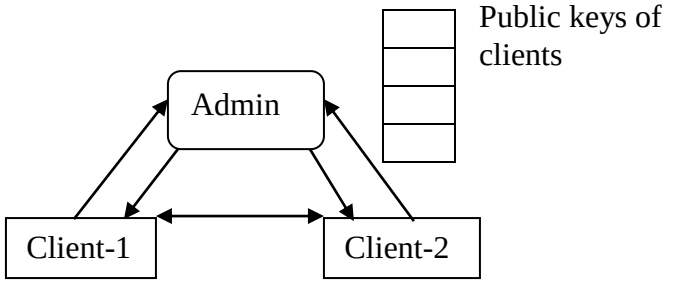

Figure 2: Secure Communication

The goal of this experiment is to use all the encryption protocols, SSL-TLS, IPSec, and Secure Layer 2 VPNs between the hosts. The student is expected to learn which applications and data can be encrypted using respective modes.

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

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: Password cracking & Recovery Lab

Explore password cracker tool 'John the Ripper' to crack the passwords in /etc/shadow file. Generate your own shadow files and crack the password.

Explore the usage of 'chnptw' tool from Kali Linux OS by booting from a Live CD or USB. Explore the possibility of resetting/bypassing the administrator password of Windows 7 user. Install Kon-Boot on USB/CD/DVD to bypass password checking procedure in Windows machine.
Use GPGPU, Rainbow Tables and CFG to crack password
Familiarize with SNORT and SURICATA. Send network packets to both the IDS and see the results

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, Perform forensics analysis on the app and document the inferences.

16CY 701 MOBILE AND WIRELESS NETWORKING AND SECURITY 2-0-1-3

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, Blue-tooth and other IEEE 802.15 standards. Mobile Computing. Threats to Wireless networks, ESM, ECM & ECCM, Privacy Challenges, Risks – Denial of Service, Insertion Attacks, Surveillance, War Driving, Jamming and Denial of Service. Authentication**,** Encryption/Decryption in GSM, GPRS & UMTS. 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. H. Chaouchi and M. Laurent-Maryline, *Wireless and Mobile Networks Security"*, Weily, 2009.
2. K. Pahlavan and P. Krishnamurthy, *Principles of Wireless Networks*, Prentice Hall, 2006.
3. C. Peikari and S. Fogie, *Maximum Wireless Security*, Sams, 2002.
4. W. Stallings, *Wireless Communications and Networks*, Second Edition, Pearson Education Ltd, 2009.
5. J. Edney and W. A. Arbaugh, *Real 802.11 Security: Wi-Fi Protected Access and 802.11i*, Addison-Wesley Professional, 2003.

16CY 702 LANGUAGE-BASED SECURITY 2-0-1-3

General purpose languages, Domain Specific languages, Abstract Syntax Tree, Axiomatic semantics of programming languages, Assertions, Tree patterns expressing security properties using discrete structures and Logic, Examining AST using ASTLOG, Querying AST objects using QL, Semmle QL Tool, Insight into Analysis and Verification of concurrent programs and cryptographic protocols written in C, Insight into Code analysis and Program Transformation using Spoon for Java. Software engineering practices for development of high assurance code - Model Checking, Program Analysis techniques for analyzing software – Static analysis, Dynamic analysis, Taint analysis, Program slicing.

TEXT BOOKS/REFERENCES:

1. M. Bishop, *Computer Security: Art and Science*, Addison-Wesley, 2012.
2. D. Kozen, *Language- based Security*, Mathematical Foundations of Computer Science 1999.
3. R. Pawlak, M. Monperrus, N. Petitprez, C. Noguera and L. Seinturier, *SPOON: A Library for Implementing Analysis and Transformations of Java Source Code*, *Software: Practice and Experience*, Wiley- Blackwell, 2015.

16CY 703 NETWORK SECURITY 2-0-1-3

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

TEXT BOOKS/REFERENCES:

1. E. Rescorla, *SSL and TLS: Designing and Building Secure Systems*, Addison-Wesley Professional, 2000.

2. T. H. Ptacek and T. N. Newsham, *Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection*, Secure Networks Inc., 1998.
3. P. Paul, *The Practical Intrusion Detection Handbook*, Third Edition, Prentice-Hall, Englewood Cliffs, 2001.
4. C. Kaufman, R. Perlman and M. Speciner, *Network Security: Private Communication in a Public World*, Second Edition, Prentice Hall PTR, 2002.
5. W. Stallings, *Network Security Essentials: Applications and Standards*, Fourth Edition, Pearson Prentice Hall, 2010.

16CY 704 STEGANOGRAPHY AND OBFUSCATION 2-0-1-3

Steganographic security, Data hiding in raw images, JPEG format, J-Steg, OutGuess. Steganalysis based on machine learning, ROC curves. Data hiding in digital Audio and Video, Operating System Data Hiding, Virtual Data Hiding, Data Hiding in Network Protocols, Forensics and Anti-Forensics, Mitigation Strategies. Code Obfuscation, Applications of Code Obfuscation. DRM, Watermarking applications and properties, Models of watermarking, Modeling Watermark Detection by Correlation. Visual Cryptography, Attacks and benchmarks for data hiding systems, Data Hiding among Android Mobile Devices and Apple iOS.

TEXTBOOKS/ REFERENCES:

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

16CY 705 INFORMATION SECURITY AND RISK MANAGEMENT 3-0-0-3

Information Risk Management, Relationships among different security components - threat agent, vulnerability, risk, asset, exposure and safeguards. Governance models such as COSO and CobiT, ISO 27000 series of standards for setting up security programs, risk analysis and management, policies, standards, baselines, guidelines and procedures as applied to Security Management program, Information strategy objectives, Security awareness and training. Security Architecture and Design – review of architectural frameworks (such as Zachman and SABSA), concepts of Security Models (such as Bell-LaPadula, Biba and Brewer-Nash), vulnerabilities and threats to information systems (such as traditional on-premise systems, web based multi-tiered applications, distributed systems and cloud based services), application of countermeasures to mitigate against those threats and security products evaluation. Business Continuity and Disaster Recovery- Business Continuity Management concepts, Business Impact Analysis, BC/DR Strategy development, backup and offsite

facilities and types of drills and tests. An introduction to Operational Security and Physical Security aspects.

TEXT BOOKS / REFERENCES:

1. A. Calder and S. G. Watkins, *Information Security Risk Management for ISO* 27001 */ISO* 27002, IT Governance Ltd, 2010.
2. S. Snedaker, *Business Continuity and Disaster Recovery Planning for IT Professionals*, Elsevier Science & Technology Books, 2007.
3. H. F. Tipton and M. Krause, *Information Security Management Handbook*, Volume 1, Sixth Edition, Auerbach Publications, 2003.

16CY 706 HDL AND CRYPTOGRAPHIC APPLICATIONS 2-0-1-3

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

TEXT BOOKS/REFERENCES:

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

16CY 707 CODING AND INFORMATION THEORY 3-0-1-4

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. S. Lin and D.J. Costello, *Error Control Coding – Fundamentals and Applications*, Second Edition, Pearson Education Inc., NJ., USA, 2004.
2. R. E. Blahut, *Algebraic Codes for Data Transmission*, Cambridge University Press Cambridge, UK, 2003.
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 and Sons, 2012.

16CY 708 SECURITY IN CLOUD COMPUTING 3-0-1-4

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. T. Mather, S. Kumaraswamy and S. Latif, *Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance*, O'Reilly Series, 2009.
2. T. Erl, R. Puttini and Z. Mahmood, *Cloud Computing: Concepts, Technology & Architecture*, Prentice Hall, 2013.
3. 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.
4. J. Dean and S. Ghemawat, *Map Reduce: Simplified Data Processing on Large Clusters*, Commun., ACM 51, no.1, 107-113, 2008.
5. 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.

16CY 709 DESIGN AND ANALYSIS OF ALGORITHMS 3-0-1-4

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

TEXT BOOKS/REFERENCES:

1. T. Cormen, C. Leiserson, R. Rivest and C. Stein, *Introduction to Algorithms*, Third Edition, McGraw-Hill, 2009.
2. R. Motwani and P. Raghavan, *Randomized Algorithms*, Cambridge University Press, 1995.
3. J. J. McConnell, *Analysis of Algorithms: An Active Learning Approach*, Jones & Bartlett Publishers, 2001.
4. D. E. Knuth, *Art of Computer Programming*, Vol. 3, *Sorting and Searching*, Second Edition, Addison-Wesley Professional, 1998.
5. S. Dasgupta, C. H. Papadimitriou and U. V. Vazirani, *Algorithms*, McGraw-Hill, 2008.

16CY 710 FORMAL METHODS FOR SECURITY 2-0-1-3

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

TEXT BOOKS/REFERENCES:

1. M. Ruth and M. Ryan, *Logic in Computer Science - Modelling and Reasoning about Systems*, Cambridge University Press, 2004 .
2. Edmund M. Clarke, Orna Grumberg and Doron Peled, *Model Checking*, MIT Press, 1999.
3. G. Bella, *Formal Correctness of Security Protocols*, Springer, 2009.
4. 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.
5. Lloyd, J.W., *Logic and Learning: Knowledge Representation, Computation and Learning in Higher-order Logic*, Springer Berlin Heidelberg, 2003.

16CY 711 SECURE SYSTEMS ENGINEERING 2-0-1-3

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

cost-benefit trade-offs.

TEXT BOOKS/REFERENCES:

1. Anderson R, *Security Engineering: A Guide to Building Dependable Distributed Systems*, New York Wiley Computer Publishing, 2001.
2. M. Tehranipoor and C. Wang, *Introduction to Hardware Security and Trust*, Springer, 2011.
3. S. Garfinkel and L. F. Cranor, *Security and Usability: Designing Secure Systems That People Can Use*, O'Reilly, 2008.
4. C. W. Axelrod, *Engineering Safe and Secure Software Systems*, Artech House, 2013.

16CY 712 SECURITY IN INTERNET OF THINGS 2-0-1-3

Internet of Things, Applications and Domain specific IOTs, IOT Protocol convergence and standardization, IOT Security, Privacy and Integration Framework, Threat Modelling and Risk assessment of IOT Product Development, Raspberry PI with Java, Raspberry PI interfaces, Connecting Raspberry PI with RFID Reader, Programming Raspberry PI with Python Packages, Sweet Security- Creating a Defensible Raspberry PI, Augmented Reality, Building a motion capture security system using Raspberry PI.

TEXT BOOKS/REFERENCES:

1. A. Bahga and V. Madisetti, *Internet of Things: A Hands-on Approach*, Universities Press (India), 2015.
2. S. Chin and J. L. Weaver, *Raspberry Pi with Java: Programming the Internet of Things*, McGraw- Hill Osborne, 2015.

16CY 713 ANDROID SECURITY 2-0-1-3

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