AMRITA
VISHWA VIDYAPEETHAM
DEEMED TO BE UNIVERSITY

School of Engineering
Amritanagar P.O., Ettimadai,
Coimbatore - 641 112 Tamil Nadu, India Ph: +91 422 2685000
Fax: +91 422 2686274 Email: ase@amrita.edu

M.TECH CYBER SECURITY SYSTEMS NETWORKS

CURRICULUM & SYLLABUS 2021

M.TECH. CYBER SECURITY SYSTEMS AND NETWORKS

Amrita Centre for Cyber Security Systems and Networks

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

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

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

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

Program Objectives (i.e. PO):

PO1: An ability to independently carry out research /investigation and development work to solve practical problems.

PO2: An ability to write and present a substantial technical report/document.

PO3: Students should be able to demonstrate a degree of mastery over the area as per the specialization of the program. The mastery should be at a level higher than the requirements in the appropriate bachelor program

Program Specific outcomes (PSOs)

PSO1: Develop good grasp of the anatomy of attacks and emerging threats within computer networks, cyber physical systems, internet of things etc.

PSO2: Design and develop fundamental building blocks and tools and/or techniques to detect and protect both digital and physical assets that are vulnerable and susceptible to cyber-attack

PSO3: Plan and prepare methods for protection of information while in process, handling, storage & transit to safeguard privacy of data

PSO4: Learn and apply data centered methods in Cybersecurity towards characterization and analysis.

List of courses Semester wise

Table1: FIRST SEMESTER

Course Code	Type	Course	L-T-P	Credits
21SN601	SC	Modern Web Application Development and Exploitation	2-0-2	4
21SN602	FC	Secure Coding and Programming	2-0-2	4
21SN603	FC	Computer Networks and Security	3-0-1	4
21SN604	SC	Cryptography and Applications	3-1-0	4
21SN605	SC	System Security	3-0-1	4
21HU601	HU	Amrita Values Program	P/F	
21HU602	HU	Career Competency I	P/F	
		Total Credits		20

Table 2: SECOND SEMESTER

Course Code	Type	Course	L-T-P	Credits
21SN611	SC	Cyber Forensics and Incident Response	3-0-1	4
21SN612	SC	Reverse Engineering and Malware Analysis	2-0-2	4
21RM606	SC	Research Methodology	2-0-0	2
	E	Elective I		3
	E	Elective II		3
	E	Elective III		3
21HU603	HU	Career Competency - II	0-0-2	1
21LIV605	HU	Live-in-Labs	P/F	
		Total Credits		20

Table 3: THIRD SEMESTER

Course Code	Type	Course	L-T-P	Credits
	E	Elective IV		3
21SN798		Dissertation	P	10
		Total Credits		13

Table 4: FOURTH SEMESTER

Course Code	Type	Course	L-T-P	Credits
21SN799		Dissertation	P	16
			credits	16

Total credits 69

Table 5: LIST OF ELECTIVES

Course Code	Type	Course	L-T-P	Credits
21SN631	E	Security Operations	3-0-0	3
21SN632	E	Cloud and Infrastructure Security	3-0-0	3
21SN633	E	Cybersecurity Governance	3-0-0	3
21SN634	E	Machine Learning for Cybersecurity	2-0-1	3
21SN635	E	Mobile Security and Vulnerability Analysis	2-0-1	3
21SN636	E	Ethical Hacking	1-0-2	3
21SN637	E	Vulnerability Analysis and Penetration Testing	0-0-3	3
21SN638	E	Hardware Security	3-0-0	3
21SN639	E	Blockchains and Decentralized Applications	2-0-1	3

21SN640	E	Security of Internet of Things	1-0-2	3
21SN641	E	Advanced Network Security	3-0-0	3
21SN642	E	Advanced Cryptography	2-1-0	3
21SN643	E	Game Theory & Its Applications to Security	3-0-0	3
21SN644	E	Advanced Android Security & Penetration Testing	1-0-2	3
21SN645	E	Data Analytics for Security	2-0-1	3
21SN646	E	SCADA Network Security	3-0-0	3
21SN647	E	Cyber Law and Privacy		3
21SN648	E	Formal Methods	3-0-0	3
21MA612	E	Mathematical Foundations of Cybersecurity	3-0-0	3
21SN649	E	Wireless Security	3-0-0	3
21SN647	E	Cyber Law and Privacy	3-0-0	3

21SN601 Modern Web Application Development and Exploitation 2-0-2-4

Introduction - Overview of web architecture, Protocols, Client server architecture, P2P architecture, DNS etc. Understanding the browser : Same origin policy, Cookies, Cache, authentication. Website development basics, understanding server side languages like nodejs, Go, client side languages such as HTML, Javascript, ReactJS, VueJs and Database languages such as SQL and nosql. Understanding the frontend, backend, database paradigm of modern web application development. Injection attacks : SQL injection, OS Command injection., LDAP Injection File upload vulnerability : LFI, RFI, how to properly secure a file inclusion vulnerability. Request forgery vulnerability : Server side request forgery, Client side request forgery. Cross site scripting attacks : Reflected XSS, Stored XSS, Dom based XSS, Self XSS, Mutated XSS, how to properly secure against XSS attacks. Server side templates and template injection, DOS & DDOS attacks, Phishing attacks, OWASP Top 10 vulnerabilities, OAuth vulnerabilities. Automating vulnerabilities. OWASP Top 10: Broken Authentication, Sensitive Data Exposure, XML External Entities, Broken Access Control, Security Misconfiguration, Insecure Deserialization, Using Components with Known Vulnerabilities, Insufficient Logging & Monitoring. Privacy laws: GDPR etc Privacy in web: Trackers, Browser fingerprinting, tor/onion network, browser extensions. Responsible vulnerability disclosure : CVE's, CVEmitre, Exploit-db, SearchSploit, bug bounty. Secure coding practices : blacklisting, whitelisting, user input validation, automated testing, trusted types, sanitizing HTML

TEXTBOOKS / REFERENCES:

1. Peter Yaworski, "Real-World Bug Hunting: A Field Guide to Web Hacking"
2. Michal Zalewski, "The Tangled Web: A Guide to Securing Modern Web Applications"
3. Dafydd Stuttard and Marcus Pinto, "The Web Application Hacker's Handbook" Second edition, 2011
4. OWASP, "Web Security Testing Guide", Fourth edition

Course Objectives

CO1. Understanding the basic concepts behind modern web architecture and development along with a solid understanding of protocols that power them.

CO2. Familiarization basic concepts such as authentication, state management in context of the application layer of web sites and applications

CO3. Learn about the various web application related vulnerabilities such as SQLi, LFI, XSS etc, the ways in which they can be exploited and how to properly secure against them

21SN602 Secure coding and programming 2-0-2-4

Fundamentals- Variables (are labels in python), Data-types: integers, strings, booleans, Control flow:Loops: while/for, if/else/elif, Containers: Lists (mutable), Dictionaries -- hashmap (mutable, but key must be hashable), Tuples (mutable), Set/frozenset, Debugging with IDE debugger, Functions, Recursive functions. Algorithms - Search-Linear search, Binary search, Sorting-Merge sort, Quick sort, Binary Search Trees, OOP-object oriented programming-Classes: attributes, methods, Inheritance. Libraries and Packages-OS: path, subprocess, files, folders I/O, Cryptography : Hashlib, fernet, secrets, CSPRNG, Netwo rking: Sockets, SSL, Web HTTP API : requests, beautiful soup, selenium, Data visualization: matplotlib, pandas, seaborn. Secure design principles. Principle of least privilege, Weakest link principle, Security through obscurity, Common Weakness Enumeration (CWE), CWE category: Memory Buffer Errors, CWE category: Bad Coding Practices, CWE category: Authentication Errors, CWE category: Authorization Errors, Secure web programming (Concurrent with Modern Web Application Development & Security), OWASP Top 10 web application security risks and their mitigations, Injection, Broken authentication, Sensitive data exposure, XML External Entities (XXE), Security misconfiguration, Cross Site Scripting (XSS), Insecure Deserialisation, Using components with known vulnerabilities, Insufficient logging and monitoring, Mapping Owasp Top 10 to application security, Mitigating application vulnerabilities (Concurrent with OS & System Security), Buffer overflow, Format string, Integer overflow

TEXTBOOKS / REFERENCES:

1. https://automatetheboringstuff.com/ (free online version)
2. realpython.com (free articles only)
3. https://jakevdp.github.io/PythonDataScienceHandbook/ (free online version)
4. CWE - CWE-1218: Memory Buffer Errors (4.4)
5. CWE - CWE-1006: Bad Coding Practices (4.4)
6. CWE - CWE-1211: Authentication Errors (4.4)
7. CWE - CWE-1212: Authorization Errors (4.4)
8. Table of Contents | OWASP

Course Objectives

CO1. Students will learn the fundamentals of computing, data structures, and algorithms

CO2. Students will be comfortable using python to automate simple tasks with OOP python scripts.

CO3. Students will know to debug their programs

CO4. Students will be familiarized with the simplicity of the python ecosystem (packages and libraries) to assist and solve many cybersecurity tasks.

CO5. Students will be able to write secure code to defend against common vulnerabilities and known exploits.

21SN603 Computer Networks and security 3-0-1-4

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

TEXTBOOKS/ REFERENCES:

1. James F Kurose and Keith W Ross "*Computer Networks – A topdown approach"*, Pearson – 7th Edition, 2017
2. Douglas E Comer " *Internetworking with TCP/IP – principles, protocols and architectures – Volume I"* -
3. William Stallings, "*Network Security Essentials - Applications and Standards*", Sixth Edition, Pearson, 2017.
4. William R Cheswick, Steven M Bellovin, Aviel D Rubin *"Firewalls and Internet Security - Repelling the Wily Hacker"*
5. Kaufman, Perlman, and Speciner.*" Network Security: Private Communication in a Public World", Second Edition, Prentice Hall PTR*

Course Outcomes

CO1 : Describe and demonstrate networking architecture and protocols

CO2 : Design and develop application specific modifications to protocols and routing

CO3 : Explain the fundamentals of security and cryptography

CO4 : Demonstrate protection of each layer with an example protocol

CO5: Design and develop intrusion detection and prevention systems, firewalls

CO6: Problem solving in network security and familiarise with research

21SN604 Cryptography and Applications 3-1-0-4

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

Unit 2: Symmetric Key Cryptographic Systems: Caesar and affine ciphers, mono-alphabetic substitutions, transposition, homophonic, Vigenere and Beaufort ciphers, one-time pad, product/iterated/block ciphers, DES and AES. Heavy discussion is given to the security of these ciphers, not only are they studied in an algorithm sense but their attacks and defences are also discussed, modes of operation: CBC, ECB.Unit 3: Cryptanalysis of symmetric keys- Attack Models, Linear, Differential and various others such as meet-in-the-middle attack .PKCS- Concepts of PKCS, Diffie Hellman key-exchange protocol, RSA, Rabin and EL Gamal cryptosystems.

Unit 4: Stream Ciphers and Digital Signatures- synchronous, self-synchronizing attack ciphers, linear feedback shift registers, Digital Signatures-RSA, multiple RSA and ElGamal signatures, digital signature standard.

Unit 5: Hash Functions and MACs- Hash functions: the Merkle-Damgard construction, Message Authentication Codes, security of Hash functions, security weakness of MD4, MD5, SHA1,SHA2, construction of SHA3.

Unit 6: Basic elliptic curve cryptography: definition, mathematical formulation of them, elliptic curve cryptography and pairings, elliptic digital signature algorithm, advantages, implementation of elliptic curve cryptography, point addition, point doubling, elliptic diffie hellman key exchange.

Unit 7: Key exchange protocols, Kerberos, Certificates, Man-in-the-middle-attack, Public key infrastructures

TEXTBOOKS/ REFERENCES:

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

Course Objectives

CO1: Understanding the mathematics behind cryptography and how to use the theorems for research purposes (PO1, PSO4)

CO2: Learn Symmetric key cryptography and the advantages and disadvantages, how to build stream ciphers and detect the weaknesses and attacks (PO1, PO2, PSO4, PSO3)

CO3: Implementation of DES, AES Algorithm and the corresponding attacks existing on them (PO1, PO3, PSO1 PSO3, PSO4)

CO4: Public key Cryptography advantages as well as various existing algorithms are explored, their proofs and how to currently attack them if implemented incorrectly. (PO1, PO2, PO3, PSO1, PSO3, PSO4)

CO5: Understand basic points of Elliptic Curves and calculate point addition and doubling (PO1, PSO2)

CO6: Understand the difference between Digital Signatures and MACs, as well as the different algorithms existing plus their corresponding weaknesses (PO1, PO2, PO3, PSO3)

CO7: Learn about Hash functions properties, how to construct strong hash function and history of hash functions, as well as constructing SHA-1 (PO1, PO2, PO3, PSO2, PSO4)

21SN605 System Security 3-0-1-4

Basic operating system concepts - Processes, Threads, Virtual memory, File system

Security Goals, Secure Design Principles, Authentication, Linux Password scheme, Password Security, Authorization - Access control, MAC, DAC, ACL, Capabilities, Information flow control, Privilege Escalation Attacks, constraining and sandboxing users and applications. Assembly Primer, Shell coding, ELF File Format. Memory Exploits – Buffer Overflow, Off by one overflow, Format String Attacks, Integer Overflow, Return to Libc, Heap Overflow, Exploit prevention mechanisms : stack canaries, Data Execution Prevention, Address Space Layout Randomization, bypassing DEP & ASLR. Trusted Execution Environment - Case Study on Intel SGX. Fuzzing - Types of fuzzers, Bug detection, Case study - AFL fuzzer. Vulnerability and exploit analysis: spectre, meltdown, foreshadow, dirty COW.

TEXTBOOKS / REFERENCES:

1. Andrew S. Tanenbaum, “Modern Operating Systems”, Fourth Edition, Pearson Education India, 2016
2. Neil Daswani, Christopher Kern, Anita Kesavan, “*Foundations of Security, What Every Programmer Needs to Know*”,Apress, 2007
3. James C. Foster and Vincent T. Liu, “*Writing Security Tools and Exploits”*, Syngress Publishing
4. Gary McGraw, John Viega, “*Building Secure Software”*, Addison-Wesley Professional, 2001.
5. Jon Ericson, “*Hacking: The Art of Exploitation”*, Second Edition, No Starch Press, 2008, ISBN 978-1593271442
6. Chris Anley, John Heasman, Felix Linder, Gerardo Richarte, The Shellcoder’s Handbook : Discovering and Exploiting Security Holes, Second Edition, Addison-Wiley, ISBN 978-0470080238

Course Objectives

CO1. A quick refresher to the fundamentals of Operating Systems

CO2. Describe security goals and principles which is used in designing a secure system (PO2, PSO2, PSO3)

CO3. Explain the basics of system organization, assembly language and linux system calls. (PO3, PSO2, PSO4)

CO4. Demonstrate the exploitation of Access control vulnerabilities and develop its mitigation (PO1, PO3, PSO1, PSO2, PSO3)

CO5. Demonstrate buffer overflow attack,Format string attack and Return to libc attack with examples (PO1,PO2, PO3, PSO1, PSO2, PSO4)

CO6. Explain the preventive mechanisms for different exploits (PO1,PSO1, PSO2)

21SN611 Cyber Forensics and Incident Response 3-0-1-4

Introduction to Cyber Forensic Investigation, Investigation Tools, Digital Evidence Collection, Evidence Preservation, Data Recovery, Encryption and Decryption methods, Search and Seizure of Computers and devices, Recovering deleted evidences, Password Cracking, Security Standards, Cyber Laws and Legal Frameworks, Cyber laws in India, Case studies and tools.

Hardware/Device/SSD Forensics, File System Forensics, OS Forensics (Windows, Linux, Android and iOS), Memory Forensics, Browser Forensics, E-Mail Forensics, Mobile/Wireless Forensics, Network and Communication Forensics, Anti-forensics, Steganography and Image File Forensics, Social media Forensics, Cloud Forensics, Overwriting/Forging/Wiping/Destruction, Obfuscation, Online Anonymity and Rootkits, Assessing Threat Levels, Operating System Attacks, Malware Analysis, Financial Frauds, Espionage and Investigations, Investigating copiers, IVR, Video surveillance, RFID and Sim cards.

TEXTBOOKS/ REFERENCES:

1. File System Forensic Analysis by Brain Carrier ISBN: 978-0-32-126817-2
2. Incident Response and Computer Forensics, Third Edition by Jason T Luttgens, Mathew Pepe ISBN: 978-0-07-179869-3
3. Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software by Michael Sikorski, Andrew Honig ISBN: 978-1-59327-290-6
4. Android Forensics: Investigation, Analysis and Mobile Security for Google Android by Andrew Hoog, ISBN: 978-1-59749-651-3
5. iPhone and iOS Forensics: Investigation, Analysis and Mobile Security for Apple iPhone, iPad, and iOS Devices by Andrew Hoog, Katie Strzempka ISBN: 978-1-59749-659-9

Course Outcomes

CO1. Exploring Cyber Forensic Investigation, Investigation Tools, Digital Evidence Collection, Evidence Preservation, Data Recovery, Encryption and Decryption methods

CO2. Familiarizing with Hardware Forensics - Disk, SSD, Memory and Mobile Forensics

CO3. Exploring the Host/OS (MS Windows, Linux, Android and iOS) Forensics and related File System Forensics

CO4. Understanding Database Forensics, E-Mail Forensics, Browser Forensics, Social Media Forensics and Anti-forensics

CO5. Exploring Network, Wireless and Cloud Forensics

CO6. Familiarizing with Cyber Laws, Regulations - Compliance & Standards

21SN612 Reverse Engineering and Malware Analysis 3-0-0-3

Low level assembly programming, identify common techniques and approaches for basic reverse engineering, disassembler and debugger aided debugging, reverse engineering high level languages, identifying and defeating anti-disassembly techniques, anti-debugging techniques, code obfuscation.Windows PE file format overview, Windows API &amp; COM overview, Malware persistence mechanisms (Registry by means of service, Trojans, DLL load order hijacking), user-mode rootkits, Privilege elevation mechanisms used by malwares, Malware execution(DLL injection, Process replacement, using Hooks and APC), Malware data encoding (common ciphers, custom encodings, Anti-analysis tricks used by malwares(Anti-disassembly, anti-debugging), Packers YARA rules, Analysing malwares.

TEXTBOOKS / REFERENCES:

1. Michael Sikorski and Andrew Honig, “ *Practical Malware Analysis*”, No Starch Press,2012
2. Bruce Dang, AlexandreGazet, Elias Bachaalany and SebastienJosse, Practical Reverse Engineering, First Edition, Wiley Publishers, 2014.
3. EldadEilam, Reversing: Secrets of Reverse Engineering, Wiley Publishers, 2005.

Course Outcomes

CO1: Understanding how to pick apart obfuscated systems systematically to understand their inner workings using reverse engineering techniques (PSO2)

CO2: Learn how to detect malicious programs and classify them from benign programs and how malicious programs try to evade detection(PSO1,PSO2)

CO3: Learn how to analyze and detect techniques used by malicious programs for activities such as persistence, data exfiltration etc(PSO1,PSO3,PSO4)

CO4: Understand how to analyze and defeat techniques used by programs such as anti debugging and anti disassembly to make their analysis (static/dynamic) harder (PSO4,PSO2,PSO1)

21RM606 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, Understanding Theory, Exploratory vs. Confirmatory Research, Experimental vs Theoretical Research, Importance of reasoning in research (Critical thinking vs plagiarism), Integrity 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, Navigating research databases.Unit III: Experimental research: Understanding valid, scientific ways to test a hypothesis, Development and writing of Hypothesis, Measurement Systems Analysis, Validity of experiments, Statistical Design of Experiments, Field Experiments, Data/Variable Types & Classification, Data collection, Data Visualisation (charting, graphing) (Documentation and Communication skills), Numerical and Graphical Data Analysis: Sampling, Observation, Surveys, Inferential Statistics, and Interpretation of Results.Unit IV: Writing skills: Preparation of 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, familiarity with systems of Error checking: Fact checking, Grammar and language checking, peer checking, review quality.Unit V: Presentation skills, condensing research in digestible ways, viewing format, smooth delivery of project to uninformed audiences, confidence building, Intellectual property rights (IPR) - patents-copyrights-Trademarks-Industrial design geographical indication. Career skills:

RM is a rigorous technical writing course that is constantly updated to suit the current needs and abilities of students. Students learn multiple skills in designing, conducting and presenting research across various mediums; be it via virtual presentations or writing or on technical writing platforms. In addition, they are taught to exercise critical thinking skills to further the research in their chosen field. Instructors aim to widen and deepen students' knowledge while also equipping them to think creatively and write Ethics of Research- Scientific Misconduct- Forms of Scientific Misconduct, Plagiarism, Unscientific practices in thesis work, Ethics in science effectively.

TEXT BOOKS/ REFERENCES:

1. Bordens, K. S. and Abbott, B. B., "Research Design and Methods – A Process Approach", 8thEdition, 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

Course Objectives

CO1. Academic Writing
CO2. Effective Communication
CO3. Academic Editing
CO4. Reading Comprehension
CO5. Data Visualization
CO6. Critical Thinking

21SN631 Security Operations 3-0-0 3

Information security incident management (Incident detection, triage and incident categories, Incident severity, resolution, Closure, Post-incident), Security Operations Center (SOC) Generations (First-generation, second, third and fourth generation SOC), SOC Maturity models (Introduction to maturity models, and applying maturity models in SOC), SOC Technologies-1 (Data collection and analysis, syslog protocol), SOC Technologies-2 (Telemetry Data, Security analysis, Data enrichment), Vulnerability Management (Broad introduction), Threat intelligence (Broad introduction), Assessment of SOC capabilities (Business and IT Goals, Assessing capabilities & IT processes), SOC - Business Continuity, Disaster recovery (Importance of BCP and DR processes, and its interface to SOC), Security event generation and collection (Cloud Security, IDPS, Breach Detection), SOC and SIEM – Introduction (Role of SIEM in SOC), SOC and Splunk (Splunk architecture & SOC, Splunk Rules, Splunk log management, Splunk correlation), SOC and Health Care - A Case study (SOC Considerations for a HealthCare situation), SOC and Application security (OWASP, Application security and SOC).

TEXTBOOKS / REFERENCES:

1.Security Operations Center: Building, Operating, and Maintaining Your SOC

Book by Gary McIntyre, Joseph Muniz, and Nadhem AlFardan

2. Designing and Building Security Operations Center, 2015

Book by David Nathans

3. Security Operations Center - SIEM Use Cases and Cyber Threat Intelligence, 2018

Book by Arun E Thomas

4. The Modern Security Operations Center, 2021

Book by Joseph Muniz

5. Principles for Cyber Security Operations, 2020
   Book by Hinne Hettema

Course Outcomes

CO1 : Students should be able to understand the functionalities of various SOC generations

CO2: Understand different data collection, data analysis and security analysis techniques as part of SOC technologies

CO3: Understand the vulnerability management techniques and threat intelligence methodologies

CO4: Assess the SOC capabilities using different SOC tools and techniques

CO5: Learn how SOC helps in business continuity and disaster recovery plan

CO5: Gain knowledge on SIEM tools with SOC compatibility

CO6: Understand SOC Considerations for HealthCare situations

CO7: Gain knowledge on the application security area with SOC

21SN632 Cloud and Infrastructure Security 2-0-1 3

Cloud computing essentials: - Characteristics, cloud computing models, service models, deployment models, NIST reference architecture, virtualization, containers, popular cloud platforms, open source architectures. Attacks in various layers of cloud computing. Threats classification and counter measures: - Infrastructure and host threats, service provider threats, generic threats, threats assessment, CSA Top threats. Risk in cloud computing: assessment, risk and trust models, security SLA. Protecting Data in the Cloud:- Tokenization, Cryptographic key management for data protection, homomorphic encryption. Vulnerability management: - Differences from traditional IT, vulnerable areas, finding and fixing vulnerabilities. Cloud computing security architecture: - general issues, trusted cloud computing platform, identity management and access control. Cloud-centric regulatory compliance issues and mechanisms.

Lab: Familiarization of popular cloud platforms, VM creation, Container management, Storage management, Network management, Access control mechanism in computing environment, Virtual private cloud, Design and deployment of secure microservice applications, TPM, Homomorphic encryption.

References/Textbooks

1. John R. Vacca(Editor), “Cloud Computing Security - Foundations and Challenges” CRC Press, 2017

2. Ronald L. Krutz and Russell Dean Vines , “Cloud Security- A Comprehensive Guide to Secure Cloud Computing” , Wiley, 2010

3. Chris Dotson “Practical Cloud Security “, O'Reilly,2019

4. Tim Mather, S. Kumaraswamy and S. Latif, “Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance”, O’Reilly Media, 2009

Course Objectives

1. Understand the architecture and infrastructure of cloud computing along with the hands-on experience in various cloud computing platforms.

2. Identify the known threats, risks, vulnerabilities, and privacy issues in the various layers of cloud computing.

3. Understand the concepts and various methods secure data management in cloud

4. Understand the security standards, tools, regulatory mandates, audit policies and compliance requirements for Cloud based infrastructures.

21SN633 Cybersecurity Governance 3-0-0 3

Unit 1-Basics of Cyber security governance- Principles of cyber-security governance,Assessment of cyber security maturity,Theories of governance – introduction,governance – definitions and typologies.Unit 2 Governance of security operations-a. Tools, methods and processes-Vulnerability management,Threat management, Endpoint management. Intrusion detection and prevention (IDPS),Security incident management. Security operations center (SOC) and related concepts. Security metrics and governance-Measurement of governance: Metrics - concepts-Application security metrics- Network security metrics- Security incident metrics- Vulnerability metrics.Service level objectives / agreement (SLO / SLA)- NIST metrics-Unit 4- Security analytics and governance- Basics of security analytics-Threat intelligence and governance- Data driven security governance- Impact of cognitive security on security governance.Unit 5-Compliance and governance- Industry specific security compliance-Cyber security governance – HIPAA compliance for healthcare - ISO, COBITZ standards - Republic of India- NIST mandates for compliance-Security reporting basics-CISO – role and organization structure

TEXTBOOKS / REFERENCES:

1. Information Security Governance: A Practical Development and Implementation Approach, Wiley publications 2009

2. Information Security Governance, S.H. Solms, Rossouw Solms, Springer Science & Business Media

3. Internet governance in an age of cyber insecurity,2010, Council on Foreign Relations Press

4.Cyber justice : human rights and good governance for the internet, 2017,Springer

Course Outcomes :

CO1 : Understand the different methods to assess cybersecurity maturity

CO2: Understand the vulnerability management techniques and threat management methodologies

CO3: Gain knowledge on the Security Operations Center (SOC)

CO4: Understand the governance metrics (Application security, vulnerability, and network security

CO5: Know the relation between security analytics and security governance

CO6: Understand the state of Security governance in India

CO7: Understand the NIST compliance for security mandate

21SN634 Machine Learning for Cybersecurity 2-0-1-3

Python, Jupyter Notebooks, Pandas, Numpy, Matplotlib, Seaborn, Scikit-Learn. Mathematics review: derivatives, gradients, sums, products. Supervised learning: Linear regression, Decision Trees, Support Vector Machines, K-nearest neighbors, random forests, adaboost, gradient boosting, multi layer perceptrons, logistic regression. Unsupervised learning: k-means clustering, dbscan, GMM, PCA, ICA, T-SNE. Bias-variance tradeoff. Learning and validation curves. Cross validation, shuffle split, k-fold, time-series split. Random seeds. Baseline and benchmarking models. Gradient descent, regularization, feature scaling, one hot encoding, label encoding. Train-test-split. Metrics: accuracy, f1-score, precision, recall, confusion matrices. Gini impurity, information gain ration, feature ranking with multivariate and univariate methods. Hyper-parameter tuning with gridsearch and random search, bayesian optimization. Natural language processing, ngrams, bag of words, vectorizers. Pipelines in scikit-learn to avoid overfitting. Data wrangling with feature preprocessing and EDA. Machine learning for security - anomaly detection, fraud detection, malware detection, spam detection, phishing detection, IDS, and NIDS. Security of machine learning: adversarial attacks on machine learning. Data poisoning, model stealing, evasion attacks at inference time. Adversarial hardening.

Text Books and references

1. Tom M Mitchell, Machine Learning, McGraw Hill, 1997
2. Jake Vanderplas, Python Data Science Handbook, O’Reilly Media, 2016

Course Outcomes

CO1. Learn and understand what Machine learning is, including all the tools of the trade. Understand that linear algebra powers most ML.

CO2. Supervised learning, requirement for labeled data, using a loss function to guide the optimization

CO3. Learn the fundamentals of regression, using linear regression, decision trees. Difference between continuous outcomes and discrete, including appropriate metrics

CO4. Fundamentals of classification, decision trees, logistic regression, SVM’s. Neural networks. Appropriate metrics

CO5. Model validation and evaluation. Gain the skill of plotting both learning curves and model evaluation curves. Ascertain whether more complexity is required or more data.

CO6. Dimensionality reduction and clustering. Understanding PCA, and k-means clustering.

CO7. Learn to conduct anomaly detection, spam classification, automated malware classification. Security oriented machine learning tasks.

CO8. Threat modeling for machine learning, understanding adversarial attacks on vision and text. Commonly known defenses, dangers of

21SN635 Mobile Security and Vulnerability Analysis 2-0-1-3

History of smartphones, smartphone application, Android Hardware Architecture Layer, IPC Mechanism in Android, Android OS Internals – Android's Init, Zygote, Binder Activity Manager, Package Manager, Google Security Services, SELinux, verified boot, Data Encryption, ARM Trustzone. Security of Mobile Networks: Security for Wi-Fi, Telecom, Personal Area Networks, Near Field Communications - Bluetooth, NFC. Android Application development, Development Tools, Application Runtime, Application Framework, Building an App, App Components, Android Debugger, Android Package (apk). App Components - Activity, Services, Broadcast Receivers, Content Providers, Intent, Intent Receivers, Android Manifest. Linux Networking Refresher– Ports, Sockets, Java Networking, Linux/Android IPTables, Android Virtual Devices – Emulator Networking, File Systems, Android Permissions, Login Credentials, Reverse engineering of APKs - apk structure and internals, Native Libraries, System Logs. Testing and Securing - Data Storage, Cryptography, Authentication, Network API, Platform API. iOS application and app store, decrypting iOS app, iOS app static analysis.

TEXT BOOKS/REFERENCES:

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

Course Outcomes

CO1: Understand internals of Android Operating System, security model of Android and iOS (PSO1,PSO2)

CO2: Understand how to make use of relevant tools to inspect and understand working of Android and iOS application (PSO1,PSO2)

CO3: Learn how to identify vulnerable codebase and insecure configuration of application components (PSO2,PSO3)

CO4: Learn how to reverse engineer and perform advanced static analysis (PSO1,PSO4)

21SN636 Ethical Hacking 1-0-2-3

VAPT Methodology : Cyber-kill chain: Reconnaissance and Information Gathering : OSINT, Breached credentials, Subdomain brute forcing, Directory scanning. Scanning and Enumeration : Scanning and exploiting open ports and services, Scanning for potential exploits in public vulnerability databases. Exploitation Basics : Metasploit, Gaining access to machines using vulnerabilities, Custom exploitation scripts, Password brute forcing, Password spraying. Active Directory : LLMNR poisoning, SMB relays, IPv6 DNS takeovers, pass-the-hash/pass-the-password, token impersonation, kerberoasting, GPP attacks, golden ticket attacks. Maintaining access : Reverse shell, file transfer. Web Application Penetration Testing. Automated Vulnerability scanners: Nessus, NMap, Metasploit, Acunetix. Report Writing : Statements of Work, Rules of Engagement, Non-Disclosure Agreements, and Master Service Agreements

TEXTBOOKS/ REFERENCES:

TEXTBOOKS / REFERENCES:

1. Bugcrowd, “The Ultimate Guide to Penetration Testing”, 2020 edition
2. HackerOne, “Web hacking 101”

Course Objectives

CO1. Familiarization with cyber kill-chain (Reconnaissance, Scanning and Enumeration, Exploitation, Privilege escalation, Maintaining access etc)
CO2. Understanding the usage of industry standard tools used as a part of the VAPT process such as Metasploit, nmap, Nessus
CO3. Ability to perform pentest a target and generate a report based on the test

21SN637 **Vulnerability Analysis and Penetration Testing** **0-0-3-3**

VAPT Methodology : Cyber-kill chain: Reconnaissance and Information Gathering : OSINT, Breached credentials, Subdomain brute forcing, Directory scanning. Scanning and Enumeration : Scanning and exploiting open ports and services, Scanning for potential exploits in public vulnerability databases. Exploitation Basics : Metasploit, Gaining access to machines using vulnerabilities, Custom exploitation scripts, Password brute forcing, Password spraying. Active Directory : LLMNR poisoning, SMB relays, IPv6 DNS takeovers, pass-the-hash/pass-the-password, token impersonation, kerberoasting, GPP attacks, golden ticket attacks. Maintaining access : Reverse shell, file transfer. Web Application Penetration Testing. Automated Vulnerability scanners: Nessus, NMap, Metasploit, Acunetix. Report Writing : Statements of Work, Rules of Engagement, Non-Disclosure Agreements, and Master Service Agreements

TEXTBOOKS / REFERENCES:

3. Bugcrowd, “The Ultimate Guide to Penetration Testing”, 2020 edition
4. HackerOne, “Web hacking 101”

Course Objectives

CO4. Familiarization with cyber kill-chain (Reconnaissance, Scanning and Enumeration, Exploitation, Privilege escalation, Maintaining access etc)
CO5. Understanding the usage of industry standard tools used as a part of the VAPT process such as Metasploit, nmap, Nessus
CO6. Ability to perform pentest a target and generate a report based on the test

21SN638 **Hardware Security** **3-0-0 3**

Preliminaries: Algebra of Finite Fields, Mathematics of Cryptography, Fundamentals of Digital Systems, Application-Specific Integrated Circuits (ASIC), Field Programmable Gate Arrays (FPGA).Cryptography Implementation: Symmetric Cryptography- DES, AES; Asymmetric Cryptography-RSA, ECC; Cryptographic Hardware and their Implementation, Optimization of Cryptographic Hardware on FPGA

Attacks against Cryptographic Algorithms: Fault Injection & Side-channel Attacks - Basic Idea, Methodologies, Algorithms and Case Studies, Design Techniques for resilience against Fault Injection and Side-channel Attacks

Hardware Security Primitives: Physically Unclonable Functions (PUFs), PUF Implementations, PUF Quality Evaluation, Design Techniques to Increase PUF Response Quality, Attacks against PUFs

Hardware Trojans: Trojan Nomenclature and Classification, Countermeasures to prevent/detect hardware trojans, Logic testing and side-channel analysis for Trojan detection

Microarchitectural Attacks: Cache-based attacks, Attacks against Branch Prediction, Spectre, Meltdown, Rowhammer Attacks

TEXTBOOKS / REFERENCES:

1. M. Tehranipoor and C. Wang, “Introduction to Hardware Security and Trust”, Springer.
2. Debdeep Mukhopadhyay and Rajat Subhra Chakraborty, "Hardware Security: Design, Threats, and Safeguards", CRC Press
3. Ahmad-Reza Sadeghi and David Naccache (eds.): Towards Hardware-intrinsic Security: Theory and Practice, Springer.

Course Outcomes:

CO1: Understand and optimize the process of implementing cryptographic algorithms on hardware

CO2: Learn the different kinds of attacks that can be mounted against cryptographic algorithms

CO3: Learn the process of building Physical Unclonable Functions and make them resilient to attacks

CO4: Understand the different kinds of Trojans, their impact and learn the effective countermeasures for defending against them

CO5: Learn the different kinds of threats at the microarchitectural level and their corresponding countermeasures.

21SN639 Blockchains and Decentralized Applications 2-0-1-3

Blockchain History. What is a Blockchain? Do you need a Blockchain? Permission-less vs Permissioned Blockchains, Public vs Private vs Hybrid vs Consortium Blockchains, Enterprise Blockchains (Hyperledger, R3 Corda), Generation of Blockchains – Bitcoin (First), Ethereum (Second with dApps), Cosmos (Third as IOB – Internet of Blockchains) Introduction to Cryptography, Public Key Cryptography, Cryptographic primitives – Cryptographic hash functions and Digital signatures, Elliptic Curve Digital Signature Algorithm (ECDSA), Crypto-economics

Blockchain Mechanics and Optimizations – Structure, Architecture, GHOST Protocol, Mining Process, Blockchain Demos

Blockchain Consensus Algorithms – Proof-of-Work (POW), Proof-of-X (POX) – Proof-of-Stake (POS), Delegated POS (DPOS), Byzantine Fault Tolerance (BFT), Practical BFT (PBFT), Ripple Protocol Consensus Algorithm (RPCA), Unique Node Lists (UNL), Paxos & Multi-Paxos, Raft, Proof-of-Authority (POA), Proof-of-Importance (POI), Proof-of-Elapsed-Time (POET), SIEVE, Proof-of-Weight (POW), Proof-of-Burn (POB), Proof-of-Activity (POA), Proof-of-Capacity (POC), Proof-of-Deposit (POD), Proof-of-Retrievability (POR), Proof-of-Luck (POL) and Tendermint

BlockDAG & Blockless DAG Protocols – SPECTRE, PHANTOM and GHOSTDAG

Blockchain IRL – Public & Private Keys, Hot and Cold Storages, Wallets, Lite Clients & Full nodes, Miners, Block & Transaction Incentives, Mining Infrastructure, Mining Pools & Organizations

Languages & Tools – Bitcoin Scripting language, Ethereum Smart Contracts using Solidity language with Tools (ethPM / npm, Node.js, EVM, Truffle, Remix IDE, Ganache, MetaMask, web3.js etc. …) and Hyperledger Fabric Chaincodes in GO language

Anonymity, Attacks on Blockchain Networks & Wallets, Scaling of Blockchains, Future of Blockchains

Decentralized Applications: Cryptocurrencies (Internet of Money) – History, Bitcoin, Ethers & Gas (Ethereum) and Atom (Cosmos), Introduction to Altcoins & Stablecoins, DOT (Polkadot), Ripple, Stellar & IOTA, Forking of Cryptocurrencies, Attack on Digital Assets, Cryptocurrencies for the Masses, Funding Crypto development (Crowd Funding, ICO & STO), How to destroy Cryptocurrencies? Token Specifications, Non-Fungible Tokens (NFTs – Internet of Assets), Decentralized Finance (DeFi) and Decentralized Autonomous Organizations (DAO)Digital Asset applications (Cryptokitties …) and Enterprise Real-World applications

TEXTBOOKS / REFERENCES:

1. Blockchain Technology by Chandramouli Subramanian, Asha A George, Abhilash K A and Meena Karthikeyan

2. Blockchain Applications – A Hands-on Approach by Arshdeep Bahga and Vijay Madisetti

3. Bitcoin and Cryptocurrency Technologies by Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller and Steven Goldfeder

4. Mastering Bitcoin by Andreas Antonopoulos

5. Mastering Ethereum, Building Smart Contracts and dApps by Andreas Antonopoulos and Dr Gavin Wood

Course Outcomes

CO1. Exploring the fundamentals of Blockchain, Types & Generations of Blockchains, Enterprise Blockchains, Blockchain Mechanics & Optimizations and Blockchain Consensus Algorithms

CO2. Familiarizing with Blockchain IRL, Network & Wallet Attacks, Scaling and Future of Blockchains

CO3. Understanding Bitcoin, Altcoins and Forking

CO4. Exploring Ethereum, dApps – Smart Contracts and related Languages & Tools, Forking, Stablecoins, Token Specifications, NFTs, DeFi and DAO

CO5. Exploring Attack on Digital assets, Cryptocurrencies for the Masses, Funding Crypto development, How to destroy Cryptocurrencies? Digital Asset applications and Enterprise Real-World applications

CO6. Familiarizing with Hyperledger Fabric, Fabric Network, Chaincode and related Languages & Tools

21SN640 Security of Internet of Things 1-0-2-3

IoT-Architecture, Functional-Architecture, Layered model, Internet of Things Attack surface, Applied Physical Attacks-Recon and Passive Analysis, Recognizing and communicating hardware impact, Sourcing documentation and tools, Reading datasheets and inferring system functionality, Threat Modeling and System Analysis, Threat modeling when hardware is in scope, Dynamic analysis, Analyzing interconnects, Analyzing an unknown protocol, Firmware vulnerability analysis and exploitation. Static vs Dynamic analysis and tools, Dynamic analysis in-circuit vs emulator, Tooling for dynamic analysis, Reverse engineering firmware, Firmware reversing using emulation.

TEXT BOOKS / REFERENCES:

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

Course Outcomes

CO1: Understanding IoT Architectures and Attack surface (PSO1)

CO2: Learn Recon and Passive Analysis on Hardware Layer (PSO1,PSO2,PSO3,PSO4)

CO3: Learn Threat Modeling and System Analysis (PSO1,PSO2,PSO3,PSO4)

CO4: Learn Firmware Vulnerability Analysis and Exploitation (PSO1,PSO2,PSO3,PSO4)

21SN641 **Advanced Network Security** **3-0-0-3**

Module 1

Network Security – Introduction – Overview of Network Attacks
TCP Overview - Connection Setup/Teardown, Packet Sniffing, Detecting Sniffers on your network, IP Spoofing, ARP Poisoning, UDP Hijacking, Fragmentation Attack- Ping of Death, Evasion & Denial of Service, UDP Hijacking, TCP Spoofing, TCP Hijacking - Mitnick attack, Joncheray attack, SYN Flood Attack, Denial of Service Attack, Port Scanning Techniques, ICMP, ICMP Attacks – ICMP Echo Attacks, Smurf Attacks, ICMP Redirect Attacks.Module 2

Wireless Security Overview, WLAN, 802.11, Adaptive network layer – graphs and routing protocols, graph theory, routing with topology aggregation, Cellular networks, adhoc networks, routing protocols, routing, QoS routing, security in adhoc networks, cognitive networks, heterogenous networks, complex networks, MIMO.Module 3

SDN – virtual networking, network virtualisation approach, network functions virtualisation, Routing in SDN-RCP, RF IP routing, Virtual Routers as a Service (VRS) , Routing as a Service (RaaS), Cloud assisted Routing (CAR) . NFV Security-Intra and extra VNF Security, NFV security countermeasures – topology verification, securing virtualisation platform, network and I/O partitioning, state management. SDN Security – design of secure and dependable SDN platform, data plane attack and countermeasures, integration with legacy protocols, cross domain connection, openflow protocol. Module 4. Advanced topics – distributed firewall, microsegmentation , intelligence in network security – neural networks and expert systems. Application of AI in IDS. SDN based intelligent network security solutions – topology protection, DoS protection.

TEXT BOOKS/REFERENCES:

1. Charlie Kaufman, Radia Perlman and Mike Speciner, "Network Security: PRIVATE Communication in a PUBLIC world", Second Edition, Prentice Hall, 2002.

2. Savo G Glisic, "*Advanced Wireless Networks*", 3rd Edition, Wiley, 2016

3. Dijiang Huang, Ankur Chowdhary, Sandeep Pisharody, "Software-Defined Networking and Security - From Theory to Practice", CRC Press (available at Taylor &Francis), 2018

Course Outcomes:

CO1: Review of Fundamentals on network security

CO2: Understand and mitigate attacks on wireless networks

CO3 : Understand routing for networks from graph theory principles

CO4: Understand virtual networking and virtualisation of network functions

CO5 : Design of secure SDN platform, with attack mitigation

CO6: Design IDS for virtual networks and intelligent protection

21SN642 Advanced Cryptography 3-0-0-3

Unit 1: Protocols, oblivious transfer, Simultaneous contract signing, Bit Commitment, Coin flipping in a well, Zero knowledge protocols, Interactive Proof Systems(IP), Zero Knowledge Definition, Application to User Identification. Multiply part protocols, secret sharing, verifiable secret sharing, anonymous transactions, multiparty ping-pong protocols, multiparty protocols when most parties are honest.

Unit 2: Homomorphic encryption definition, goldwasser-Micali Encryption scheme, Elgamal encryption scheme, Paillier Encryption Scheme, Boneh-Goh-Nissim Encryption Scheme.

Unit 3: Fully Homomorphic encryption definition, Overview of fully homomorphic encryption schemes, secret key somewhat homomorphic encryption, public key somewhat homomorphic encryption. Fully Homomorphic Encryption scheme over images: squashed encryption, bootstapple encryption and Implementation.

Unit 4: Quantum Cryptography Introduction,Quantum Cryptography Threat and Challenges Ahead such as Analysis, Implementation and Caveats. Families of Post-quantum schemes: Code-based Cryptography, Lattice-based cryptography, Hashed-based cryptography, Multivariate Cryptography.

TEXTBOOKS/REFERENCES:

1. Xun Yi, Russel Paulet, Elisa Bertino Homophoric Encryption and Applications
2. Jonathan Katz, Yehuda Lindell Introduction to Modern Cryptography
3. Lattice Based Cryptography for Beginners Pikere’ts Bonn Lecture Slides

Course Outcomes

CO1: Understanding the various different protocols that exist and the importance of them in the real world. (PO1, PSO4)

CO2: Learn homomorphic encryption and the existing algorithms as well as their weaknesses (PO1, PO2, PSO4, PSO3)

CO3: Implementation and understanding of various full homomorphic encryption schemes (PO1, PO3, PSO1 PSO3, PSO4)

CO4: Understanding Importance of Quantum Cryptography and Post Quantum cryptography and how to approach moving to Quantum Computing (PO1, PO2, PO3, PSO1, PSO3, PSO4)

21SN643 Game Theory and its applications in Cybersecurity (Elective) 3-0-0 3

Preliminaries: Static and Dynamic Games, Normal form and Extensive Form Games, Zero-sum and Non-zero-sum games, Bayesian Games, Stackelberg Games, Perfect vs Imperfect Information, Complete vs Incomplete Information, Stochastic Games.Intrusion Detection Games: Cyber Warfare Games, Games for Denial of Service and Distributed Denial of Service (DDoS), Flooding, Malware, Ransomware. Games for Protecting Critical Infrastructure.Wireless Security Games: Physical and MAC layer security games, Secure Routing Games, Games for Secure Ad hoc, Sensor and Vehicular Networks.Economics of Cybersecurity: Games for Resource Allocation and Incentive compatibility, Games for Risk Assessment and Mitigation, Economic models and metrics for Cybersecurity.Blockchain Games: Game theoretic models for Consensus algorithms, Games for Double Spending Attacks and Selfish Mining, Cheating Games, Games for DDoS attacks.Privacy Games: Games for Identity and Location Privacy, Local vs Global Eavesdroppers, Trust Games, Trust vs Privacy

TEXTBOOKS / REFERENCES:

a) Y. Narahari, “Game Theory and Mechanism Design”, World Scientific

Course Outcomes:

CO1: Understand the different kinds of games and their applications to Cybersecurity

CO2: Learn the different facets of Intrusion detection and develop game theoretic models for modeling cyber attacks

CO3: Understand the development of game theoretic models for vulnerabilities at the Physical, MAC, routing and application layers

CO4: Understand the interplay between economics and cybersecurity and develop game theoretic models for resource allocation and incentive compatibility and evaluate them using metrics

CO5: Learn the development of game theoretic models to model the different threats in the Blockchain environment

CO6: Understand the development of games to preserve identity and location privacy from both local and global eavesdroppers.

21SN644 Advanced Android Security and Penetration Testing 1-0-2-3

Introduction to Android Authentication Architecture, Network communication, Cryptography. Reverse Engineering - Assets and resources, Application mapping with Manifest, Resources. Understanding vulnerabilities - Data Storage (logging sensitive data, insecure file management), Local databases (Encryption, Hashing), External Storage, Authentication (Validation and Authorization), Network API (SSL Certificates, HTTPS), Platform API, Exported Activities, Browsable/Custom Intents, Username enumeration, Broken Cryptography, Insecure Key Management. Traffic Analysis and interpretation. Reverse Engineering and Analyzing Native Libraries. Introduction and hands-on of tools for pentesting - frida, objection, runtime mobile security, MobSF, Adhirit, drozer, burpsuite etc, Identification and Analysis of Android Malware and Spyware. Penetration Test report writing.

TEXT BOOKS/REFERENCES:

1. Aditya Gupta, "*Learning Pentesting for Android Devices"*
2. Dominic Chell, Tyrone Erasmus, Shaun Colley, Ollie Whitehouse, *"The Mobile Application Hacker's Handbook",* ISBN: 978-1-118-95850-6, February 2015

Course Outcomes

CO1: Understand how to perform dynamic analysis and application execution behavior (PSO4,PSO2)

CO2: Understanding attack vectors and recent attacks on mobile platform (PSO2,PSO3)

CO3: Learn to perform penetration testing on Android applications (PSO3,PSO4)

CO4: Understanding packers and obfuscation techniques used in mobile Malware/Spyware/Ransomware (PSO2, PSO4)

21SN645 Data Analytics for Security 2-0-1-3

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

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

TEXTBOOKS / REFERENCES:

1) Daniel Barbara and SushilJajodia, “Applications of Data Mining in Computer Security”, Vol. 6. Springer Science & Business Media, 2002

2) Marcus A. Maloof, “Machine Learning and Data Mining for Computer Security”, Springer Science & Business Media, 2006

3) V RaoVemuri, “Enhancing Computer Security with Smart Technology”, Auerbach Publications, 2005

4) S. Stolfo, S. Bellovin, S. Hershkop, A. Keromytis, S. Sinclair, S. Smith, “Insider Attack and Cyber Security: Beyond the Hacker”, Vol. 39. Springer Science & Business Media, 2008

5) Dhruba K. Bhattacharyya, Jugal K. Kalita, “Network Anomaly Detection: A Machine Learning Perspective”, Crc Press, 2013

6) AnoopSinghal, “Data Warehousing and Data Mining Techniques for Cyber Security”, Vol. 31. Springer Science & Business Media, 2007

7) Markus Jakobsson and ZulfikarRamzan, “Crimeware, Understanding New Attacks and Defenses”, Addison-Wesley Professional, 2008

Course Outcomes

CO1: Understanding various data mining techniques for information security (PO3,PSO4)
C02: Understand and apply networking intrusion systems for detection of insider threats such as phishing emails, spam emails etc (PO1, PSO1, PSO2
CO3: Have an understanding on how to build systems that utilize behavioral biometrics along with mouse dynamics for authentication purposes (PO1, PO2, PSO3)
CO4: Apply machine learning with security (PO3, PSO4)

21SN646 SCADA Network Security 3-0-0-3

ICS Overview-Processes & Roles,Controllers and Field Devices,SCADA,Exercise: Programming a PLC & HMI. IT & ICS Differences-ICS Life Cycle Challenges,Architectures and Field Devices-ICS Attack Surface,Secure ICS Network Architectures,Exercise-Identifying External Attack Surfaces,Architecting a Secure ICS Site,Communications and Protocols-Ethernet and TCP/IP,Enforcement Zone Devices,Basic Cryptography,Wireless Technologies,Wireless Attacks and Defenses,Exercise,Enumerating Modbus TCP ,Supervisory Systems,Supervisory Servers & Attacks,User Interfaces & Attacks,Defending Services,Exercise: Bypassing Auth with SQL Injection,Fuzzing,ICS Security Governance,Defending Unix and Linux,Endpoint Protection,Measuring Cyber Security Risk,Incident Response,Exercise-Hardening Linux,Event Logs,Risk Approaches and Calculations

TEXT BOOKS / REFERENCES:

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

Course Outcomes

CO1: Understanding SCADA Architectures and learn how to program PLC and HMI (PSO2)

CO2: Understand how to Identify External Attack Surfaces and the various SCADA protocols that exist and the importance of them in the real world (PSO1,PSO3)

CO3: Learn how to automate vulnerability detection techniques and Architecting a Secure ICS Environment (PSO1,PSO2,PSO3,PSO4)

CO4: Understand different ICS Security Governance used in industry such as Hardening OS, Risk Approaches and Calculations etc (PSO1,PSO2,PSO3,PSO4)

21SN648 Formal Methods 3-0-0-3

Background: Computability and Complexity, Decidability, Semi-decidability, Undecidability, Halting problem, Rice's theorem, Overview of complexity classes: P, NP, NP-completeness. Propositional and First-Order Logic: Syntax, Semantics, Proof methods , Program Verification: Floyd-Hoare logic, Weakest Pre-conditions; Partial Correctness and Termination Structural induction and Fixed-point induction for recursive procedures
Z specification language: Fundamentals and abstract data type specifications. Data refinement in Z abstract data types: Forward and backward simulation, Concurrent Programs and Correctness Properties: Owick-Gries, Assume-Guarantee, Reactive Systems: Transformational vs Reactive systems, Temporal Logic: Linear (LTL) and Branching Time (CTL), Temporal specification of reactive systems: Safety, Liveness, Fairness, Buchi automata, LTL-to-Buchi automata, Properties: containment, emptiness, Model Checking: LTL and CTL model-checking. Analysis of model-checking algorithms Symbolic model checking; overview of state-space reduction methods, Case study and practical verification of properties, Process Algebra: CCS and Pi-calculus, Reductions and labelled transitions, Harmony lemma, Bisimulations

CO1: Get an understanding of the background in Formal Methods and learn the different types of classes.
CO2: See the different type of proof methods and apply them to Security applications
CO3: Learn about the different type of Correctness properties and know when to use them
CO4: Have a good understanding on analysis of models

TEXT BOOKS / REFERENCES:

1. E.M. Clarke, O. Grumberg, and D. Peled "*Model Checking*", 2nd Edition, MIT Press, 2018.
2. DavideSangiorgi and David Walker, "Pi-calculus: The Theory of Mobile Processes", Cambridge University Press,2003
3. SanjeevArora and Boaz Barak, "Computational Complexity – A Modern Approach", Cambridge University Press, 2017
4. Michael Huth and Mark Ryan, "*Logic in Computer Science*". 2nd Edition, Cambridge University Press, 2004.
5. J. Woodcock & J. Davies "*Using Z: Specification, Refinement and Proof"*, Prentice Hall, 1994.

21MA612 Mathematical Foundation for Cybersecurity 3-0-0-3

Unit 1: Sets, subsets, and their respective properties. Relations and their properties, functions, bijective function, inverse functions, domain, and range.Unit 2: Matrix Theory: Basic Matrix algebra, determinant of a matrix, inverse of a matrix, finding solution of a linear system, geometry representation of matrices, Subspace, Vector Space, Solution Space of a Matrix, Null-Space, Basis, Linear independent, Spanning set.Unit 3: Probability Theory: Permutations and combinations, basic probability theory, probability threes, conditional probability, Independence, Bayes Theorem, Random variable definition, discrete random variables and their properties, Bernoulli, Binomial, Uniform, probability mass function, Cumulative distribution function, expectation and Variance.Unit 4: Continuous random variables, normal distribution, exponential, geometric, PDF, CDF, Marginal distribution, Independent Random Variables, Joint Random Variable.Unit 5: Random process: general concept, power spectrum, discrete-time processes, random walks and other applications, Markov chains, transition probabilities.Unit 6: Introduction to Game Theory, basic game theory games and their application to Cyber Security

TEXTBOOKS / REFERENCES:

1) Erwin Kreyszig, "*Advanced Engineering Mathematics*", 10th Edition, Wiley ISBN: ES8-0-470-91361-1

2) Kenneth Rosen, "*Discrete Mathematics and Its Applications*", 8th Edition, 2019

3) Sheldon Ross, "*A First Course in Probability*", 10th Edition, Pearson, 2019

4) Peter Morris, "*Introduction to Game Theory*", Springer,1994

5) A. Papoulis and U. Pillai, Probability, “*Random Variables and Stochastic Processes”*, Fourth Edition, McGraw Hill, 2002.

Course Outcomes

CO1 : Understand the basic mathematical functions for cyber security

CO2 : Understand basics of matrix algebra and vector spaces

CO3 : Understand basics of probability theory and distributions

CO4: Understand usage of random variables for cryptography

CO5 : Understand usage of random and stochastic processes for cyber security

CO6: Understand basics of game theory for cyber security

21SN649 Wireless Security 3-0-0-3

Wireless Standards Security: Vulnerabilities in existing Wireless networks, Bluetooth Low Energy (BLE) Security, 3G Security, 4G Security, 5G Security, Wifi Security. Trends and Upcoming Wireless Networks: Upcoming Wireless Networks, Trends and Security challenges in wireless networks. Trust Assumptions and Adversary models: Trust, Trust in Ubiquitous computing. Physical Layer Security: Jamming, Wiretapping, Physical Layer defenses. MAC Layer Security: Operating principles of IEEE 802.11, Detecting selfish behavior in hotspots, Selfish behavior in pure ad hoc networks, MAC layer defenses. Network Layer Security: Securing ad hoc network routing protocols, Secure routing in sensor networks, Network layer defenses. Privacy in Wireless Networks: Privacy in RFID Systems, Location privacy in vehicular networks, Privacy preserving routing in ad hoc networks. Game Theory: Normal Form Games, Strict Dominance, Weak Dominance, Iterated Dominance, Pure and Mixed Strategy Nash Equilibrium, Extensive Form Games, Backward Induction, Subgame Perfect Nash Equilibrium, Game Theory in Wireless Networks, Forwarder's dilemma, Joint Packet Forwarding game, Multiple Access Game and Jamming Game. Applications: RFID Security, Security for Wireless Sensor Networks, Security for Vehicular Networks.

TEXT BOOKS/REFERENCES:

1. Levente Buttyán and Jean-Pierre Hubaux, Security and Cooperation in Wireless Networks, 2008.

Course Outcomes:

CO1: This introduces students to Wireless Security and provides a study of technical and practical aspects of Wireless networks
CO2: This introduces students to practical aspects of cryptography for application to wireless networks. A suite of techniques ranging from symmetric and asymmetric key techniques will be studied.
CO3: This course helps students to understand the security of diverse wireless networking standards. In particular, vulnerabilities and their corresponding security enhancements are presented
CO4: This course introduces students to the notion of trust in wireless networks and discusses mechanisms for enforcing trust in wireless networks
CO5: This introduces students to the security issues at the physical and MAC layers. Further, attacks that can be launched on the physical and MAC layers along with their corresponding defenses are presented
CO6: This introduces students to the security issues in the routing layer. In particular, attacks that can be launched on the network layer along with mechanisms for defending against them are presented
CO7: This introduces students to naming and addressing and discusses attacks that can be launched by leveraging the identities and network addresses. Finally, mechanisms for defending such notorious threats are presented
CO8: This introduces students to privacy in wireless networks, mechanisms for enforcing privacy in wireless networks. Finally, we discuss the integration of privacy in wireless network routing
CO9: This introduces students to security in vehicular networks. In particular, attacks against vehicular networks are presented along with existing approaches for defending against such attacks
CO10: Introduce students to the security issues in RFID and present the attacks against RFID systems. In addition, mechanisms for RFID Security are discussed.
CO11: Introduce students to non-cooperative game theory and discuss the applications of game theory for security in wireless networks

21SN647 Cyber Laws and Privacy 3-0-0-3

Evolution of Privacy Laws in India Protection, Current status of Data Protection in India PDPB 2018-Applicability, Definitions, Rights and Obligations. Penalties, Exemptions and Restrictions, Institutions under PDPA.

Indian Laws-Concept of Privacy, Data Protection and Evolution of Privacy and Data Protection Laws in India, ITA 2000, ITA (Amendment) 2008, PDPB 2018, Overview of PDPB 2019, Penalty structure, Data Protection Authority, Social media Bill 2021. Applicability and Key Definitions, Exemptions, Roles of Guardian Data Fiduciary, Significant data fiduciary, Rights of Data Principles and Obligations of Data Fiduciaries, Consent and Processing without consent, Cross Border Transfer, Transparency and Compliance Requirements, DPO Data Audits and Data breach Notification.

EU-GDPR: Applicability, exemptions, Definitions, Penalties, Rights of data subjects and Data Protection Principles Compliance Requirements, Cross border data transfer, DPIA and Data Breach Notification, some caselets.

Legal aspects of privacy, database privacy, location privacy in mobile environments, social network privacy, RFID privacy, privacy preserving transportation logistics and financial cryptography, query log and biometrics privacy for Big Data.

Fair and accurate credit transactions, children’s online privacy protection, ID Theft.

TEXT BOOKS/REFERENCES:

1. Kamath Nandan, *Law relating to Computer, Internet and E-Commerce*. Universal Law Publisher,(2012)
2. Personal Data Protection Bill from Lok Sabha “http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf”
3. IT Governance Privacy Team - *“EU- General Data Protection Regulation*” – 4th edition, IT Governance Publishing.
4. Christopher Kuner, Lee A. Bygrave, Christopher Docksey, and Laura Drechsler “T*he EU General Data Protection Regulation (GDPR): A Commentary”*, Oxford University Press, 2021

5. S. R. Bhansali, “*Information Technology Act, 2000,*” University Book House Pvt. Ltd., Jaipur (2003)

6. Jody R Westby, ”*International guide to Privacy*” - American Bar association

7. Rainer Böhme Michael Brenner, Tyler Moore, Matthew Smith, *Financial Cryptography and data security* – Springer

Course Outcomes

CO1 : Understand dimensions of Indian Cyber Law.

CO2 : Define key terms and concepts for international Cyber Laws such as GDPR

CO3 : Get the background for privacy applicable to society