Syllabus

M.Tech Computer Science and Engg.(Cyber Security)

I Semester

MAT *** Mathematical Foundations of Cybersecurity [4 0 0 4]

Abstract

Propositional logic, Propositional equivalences, Predicates and quantifiers, Proof methods, Sets, subsets, and power sets; Basics of counting, Pigeonhole principle, Permutations and combinations, Binomial coefficients and identities, Generating functions, Divisibility and Modular Arithmetic, Integer Representations and Algorithms, Applications of Congruences, Groups, rings, and fields, Linear transformations and matrix representation; Eigen values and eigen vectors, Graphs and graph models, Shortest-path problems, Planar graphs, Graph coloring, Probability theory and random variables, Discrete and continuous distributions, Bayesian inference and estimation, Markov chains and random processes.

References

1. Kenneth H Rosen, *Discrete Mathematics and Its Applications*, 8th Edition, McGraw Hill, 2021
2. Howard Anton, Chris Rorres, and Anton Kaul, *Elementary Linear Algebra: Application Version*, 12th Edition, Wiley, 2019
3. Athanasios Papoulis and s Pillai, Probability, Random Variables and Stochastics Processes,
   4th Edition, McGraw Hill Education, 2017

ICT *** Applied Cryptography [4 0 0 4]

Abstract

Introduction, Mathematics of Cryptography, Number Theory, Secret Key Cryptography: Encryption, Stream Ciphers, Block Ciphers, Chosen Plaintext Attack, Message Integrity, Authenticated Encryption; Public Key Cryptography: Public Key Tools, Public Key Encryption, Chosen Ciphertext Secure Public Key Encryption, Digital Signatures, Elliptic Curve Cryptography; Protocols: Protocols for Identification and Login, Identification and Signatures from Sigma protocols, Authenticated Key Exchange.

References

1. Jean-Philippe Aumasson, Serous Cryptography: A Practical Introduction to Modern Encryption, 2nd Edition, No Starch Press, 2024.
2. Dan Boneh and Victor Shoup, A Graduate Course in Applied Cryptography, Draft Version.06, 2023.
3. Christof Paar and Jan Pelzl, Understanding Cryptography, Springer, 2014.
4. Bruce Schneier, Applied Cryptography, Wiley, 2017.

5. Niels Ferguson, Bruce Schneier, and Tadayoshi Kohno, Cryptography Engineering: Design Principles and Practical Applications, Wiley, 2010.

ICT **** Zero Trust Security [3 0 2 4]

Abstract

Introduction to Zero Trust- Forrester's Zero Trust eXtended (ZTX) Model, Gartner's Approach to Zero Trust, Core Principles, Zero Trust Platform Requirements, Zero Trust Architectures, Zero Trust and Enterprise Architecture Components, Zero Trust In network- Network Firewalls, The Domain Name System, Wide Area Networks, Zero Trust and Access Management- Privileged Access Management, Data Protection, Data Types and Data Classification, Data Lifecycle, Data Security, Zero Trust and Data, A Zero Trust Policy Model. , Zero Trust and services, Zero Trust Scenarios.

References

1. Jason Garbis, Jerry W. Chapman, Zero Trust Security An Enterprise Guide, Apress, 2021.
2. Andrew McDonald, Brandon Fowler, Cindy Green-Ortiz, David Houck, Hank Hensel , Jason Frazier, Patrick Lloyd, Zero Trust Architecture (Networking Technology: Security), 2023

ICT *** AI for Cyber Security [3 0 2 4]

Abstract

Introduction to AI and Cybersecurity, Machine Learning Basics, Data Collection and Preprocessing, Intrusion Detection Systems, Anomaly Detection, Malware Analysis, Threat Intelligence and Prediction, Natural Language Processing in Cybersecurity, Deep Learning Applications, Adversarial Machine Learning, Case Studies and Industry Applications and Ethical and Legal Considerations.

References

1. Clarence Chio, David Freeman, Machine Learning and Security, O'REILLY, 2018
2. Clarence Chio and David Freeman, Machine Learning and Security: Protecting Systems with Data and Algorithms, O'REILLY 2018
3. Arun Kumar Krishna, AI in Cybersecurity: Transforming Threat Detection and Response, 2024
4. Leslie F. Sikos, Artificial Intelligence in Cyber Security, Springer, 2019
5. Emmanuel Tsukerman, Machine Learning for Cybersecurity Cookbook, 2019

ICT **** Principles of Secure coding [3 0 2 4]

Abstract

Introduction to secure coding, security attacks, common vulnerabilities, security policies and procedures, philosophy of secure programming, Integrating security with Software Development Design Cycle: Architecture, Design, Implementation and Automation and Testing, Compliance and legal aspects in coding, case studies. Threat modelling process and its benefits. Secure Coding Techniques. Database and Web-specific issues . Test Secure Applications.

References

1. Robert Seacord, Secure Coding: Principles and Practices, Addison-Wesley Professional, 2013
2. Chris B Behrens, Principles of Secure Coding-Mastering Secure Coding Practices for Robust Applications, 2024
3. Michael Howard and David LeBlanc, Writing Secure Code, , Microsoft Press, 2nd Edition, 2004
4. Jason Deckard, Buffer Overflow Attacks: Detect, Exploit, Prevent, Syngress,1st Edition, 2005
5. Frank Swiderski and Window Snyder, Threat Modeling, , Microsoft Professional, 1st Edition, 2004

ICT **** Applied Cryptography and Secure Coding Lab [0 0 3 1]

Experiments on symmetric and asymmetric key systems, Secure protocols, Elliptic Curve Cryptography; Protocols: Protocols for Identification and Login, Identification and Signatures from Sigma protocols, Authenticated Key Exchange.

References

1. Jean-Philippe Aumasson, Serous Cryptography: A Practical Introduction to Modern Encryption, 2nd Edition, No Starch Press, 2024.
2. Niels Ferguson, Bruce Schneier, and Tadayoshi Kohno, Cryptography Engineering: Design Principles and Practical Applications, Wiley, 2010.

ICT **** Information Security mini project [0 0 3 1]

Students are expected do a mini project with the knowledge acquired from study of various security courses.

II Semester

ICT **** Mobile and Web Application Security [3 0 2 4]

Abstract

Web Application Security: Web Applications and Web Application Security Fundamentals, Browser Security Principles, Web Application Vulnerabilities and Mitigations, Secure Website

Design, Cutting Edge Web Application Security, Mobile application security: Introduction to Mobile Security, Supervised Learning Detection of Malware on Android, Vulnerabilities in Mobile Applications, RESTful IoT Authentication Protocols, Data Privacy Models

References

1. Sullivan, Bryan, and Vincent Liu, Web Application Security, A Beginner's Guide, McGraw Hill Professional, 2011.
2. Stuttard, Dafydd, and Marcus Pinto, The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws, John Wiley Sons, 2011
3. Man Ho Au, Raymond Choo, Mobile Security and Privacy, Syngress.2016
4. Dwivedi, Himanshu; Clark, Chris; and Thiel, David. Mobile Application Security, McGraw-Hill Osborne Media, 2010.

ICT **** Digital Forensics and Incident Response [3 0 2 4]

Abstract

Introduction to digital forensics, cybercrimes, electronic evidence handling, internet crimes, hacking, and cryptography. Computing investigations, computer forensics, data acquisitions, understanding windows systems, evidence capture, usage of forensic tool, Use of slack space, disk imaging, data recovery, vulnerability assessment tools, anti-forensics. Retrieving information, processing digital evidence, and handling multimedia evidence.

References

1. C. Altheide& H. Carvey Digital Forensics with Open Source Tools, Syngress, 2011. ISBN: 9781597495868
2. Warren G. Kruse II and Jay G. Heiser, "Computer Forensics: Incident Response Essentials", Addison Wesley, 2002.
3. Nelson, B, Phillips, A, Enfinger, F, Stuart, C., "Guide to Computer Forensics and Investigations, 2nd ed., Thomson Course Technology, 2006, ISBN: 0-619-21706-5.
4. Vacca, J, Computer Forensics, Computer Crime Scene Investigation, 2nd Ed, Charles River Media, 2005, ISBN: 1-58450-389.

ICT **** Mobile and Web Application Security Lab [0 0 3 1]

Abstract

Authentication and Authorization in Web, API Security, Web Application Testing, Internal Penetration Testing, SSID or Wireless Testing, Mobile Application Testing, Hacking the Web: Tools and Techniques, Understanding android permissions and apk signing, OWASP top 10 for mobile, android log vulnerabilities, android dropbox vulnerabilities, android content stack and malicious payload analysis.

References

1. Sullivan, Bryan, and Vincent Liu, Web Application Security, A Beginner's Guide, McGraw Hill
   Professional, 2011.
2. Dwivedi, Himanshu; Clark, Chris; and Thiel, David, Mobile Application Security, McGraw-Hill Osborne Media, 2010.

ICT **** Cyber Security and Digital Forensics mini project [0 0 3 1]

Design, develop, and deploy the models of computer forensics. The project to be developed must go through all the cyber forensics phases-Assess, Acquire, Analyse and Report.

Program Electives [3 0 2 4]

ICT **** Quantum Cryptography

Abstract

Introduction to Quantum mechanics and quantum parallelism- Mathematical Model for Quantum Mechanics, Single and multi-qubit quantum gates, No cloning theorem. Quantum circuits emulate classical circuits. Quantum Parallelism, Quantum Algorithms, Deutsch-Jozsa, Simons, Bernstein-Vazirani, Grover's, Shor's, Post quantum cryptography from lattices- Introduction to lattices, Learning with Errors and Short Integer Solution problem, Quantum public key encryption, Quantum fully homomorphic encryption, lattices and quantum hardness.

References

1. M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge: Cambridge University Press, 2010.
2. A. Yu. Kitaev, A. H. Shen, and M. N. Vyalyi. Classical and Quantum Computation. American Mathematical Society, USA, 2002.
3. F. Grasselli, in Quantum Cryptography: From Key Distribution to Conference Key Agreement, Springer International Publishing, Cham, 2021.
4. Daniel J. Bernstein, Johannes Buchmann, Erik Dahmen, Post-Quantum Cryptography, , Springer International Publishing, 2009.
5. Research papers and online lecture notes
   Online resources:
6. CS 7260: Quantum and Post-Quantum Cryptography, IIT Madras, https://cse.iitm.ac.in/~shwetaag/CS7260.html
7. NPTEL Course: Quantum Algorithms and Cryptography, By Prof. Shweta Agrawal, IIT Madras, https://onlinecourses.nptel.ac.in/noc23_cs04/preview
8. Beyond the Bootcamp: CS 294-168 Lattices, Learning with Errors and Post-Quantum Cryptography, MIT, https://people.csail.mit.edu/vinodv/CS294/

ICT **** Threat Intelligence

Abstract

Introduction, the backbone of robust cybersecurity, systematic gathering, analysis, and dissemination of information on potential cyberattacks. Organizations to understand attacker motivations, tactics, and threat landscape. Data collection from security logs, threat feeds, and social media. In-depth analysis to identify patterns, trends, and indicators of compromise (IOCs). Proactive defence, incidence response, and decision on resource allocation and security control prioritization. Exploration of foundational principles, data acquisition methods, analysis techniques, and different strategic, tactical, and operational threat intelligence types. Threat intelligence reports writing and case studies.

References

1. Ali Dehghantanha, Mauro conti, tooska Dargahi, Cyber threat intelligence Springer publications, 2018
2. TestOut: CyberDefense Pro. ISBN: 978-1-935080-73-2, 2021

ICT **** Cyber Physical Systems Security

Abstract

Introduction to Industrial Control Systems and Operations, Industrial Network Protocols, Cyber Physical System Modeling, Plant Models, Feed Back Control Model, and Anomaly Detection Models, CPSS- Concepts and Principles, Securing Industrial Control Systems, Advanced Cyber-Physical Systems Security Concepts, Cyber threat model, Critical Infrastructures-Critical Infrastructures such as Power Grid, Railways Systems, Transportation Systems, Water/Sewage Systems and their automation architecture, Vulnerabilities, and Past Cases of Cyber Security Compromises, SCADA based control, Sensors (IEDs, PLCs), field network and its protocols (profibus, DNP3 etc), ICS/SCADA Security, IoT Security, Legal and Privacy Aspects, CPSS: Risk Management.

References

1. Sajal K. Das, Krishna Kant, Nan Zhang, Morgan Kaufmann , Handbook on Securing Cyber-Physical Critical Infrastructure, (Elsevier), ISBN 978-0-12-415815-3, Publication: 2012.
2. Jeeva Jose, Vijo Mathew, Introduction to Security of Cyber-Physical Systems Khanna Publishing, 2022

ICT **** Software Defined Networking Security

Abstract

Introduction to Software Defined Networking, Security Fundamentals and security challenges in SDN, Attack Vectors and Countermeasures, Security Protocols and Standards, Security in

SDN Applications, Case Studies and Practical Applications, Future Directions in SDN Security.

References

1. Paul Goransson and Chuck Black, Software Defined Networks: A Comprehensive Approach, Morgan Kaufmann Publications, 2014
2. Thomas D. Nadeau, Ken Gray, SDN: Software Defined Networks, An Authoritative Review of Network Programmability Technologies, O'Reilly Media, August 2013

ICT **** Mobile and Wireless Security

Abstract

Introduction and Security concerns to mobile and wireless security, Security of Device, Network, and Server Levels, Application-Level Security in Wireless Networks, WLAN access control and authentication mechanism, Application-Level Security in Cellular Networks, Wireless networks compromising techniques and security policy, Application-Level Security in MANETs.

References

1. Physical Layer Security in Wireless Communications (Wireless Networks and Mobile Communications) by Xiangyun Zhou, Lingyang Song and Yan Zhang .2013
2. Pallapa Venkataram, Satish Babu: "Wireless and Mobile Network Security", 1st Edition, Tata McGraw Hill,2010.
3. Wireless Security by Wolfgang Osterhage.2011
4. Mobile Application Security by Himanshu Dwivedi, Chris Clark and David Thiel. 2010
5. Y. Xiao, X. Shen, D. Z.Du, Wireless Network Security, Springer International Edition.
6. Lei Chen, JiahuangJi, Zihong Zhang, Wireless Network Security, Springer Science & Business Media

ICT **** Blockchain Technology

Abstract

Introduction to technology stack: Blockchain, protocol, understanding how blockchain works. Introduction to blockchain primitives, consensus model. Introduction to smart contracts and its development environment. Architecture of decentralized application using Ethereum and Hyperledger platforms. Introduction to Hyperledger.

References

1. Elad Elrom, The Blockchain Developer, Apress; 1st edition, 2019
2. Lorne Lantz, Daniel Cawrey, Mastering Blockchain, O'Reilly Media, Inc.2020.
3. Paul Vigma, Michael J. Casey, The Truth Machine: The Blockchain and the Future of Everything,1st edition, St Martin's Press, 2018.
4. Daniel Drescher, Blockchain Basics: A Non-Technical Introduction in 25 Steps, 1st edition, Apress, 2017.
5. Xun Brian Wu, Chuanfeng Zhang, Andrew Zhang, Hyperledger Cookbook, Packt Publishing Limited, 2019
6. David Hooper, Kevin Solorio, Hands–On Smart Contract Development with Solidity and Ethereum: From Fundamentals to Deployment, O′Reill, 2019.

ICT **** Ethical hacking

Abstract

Introduction to Hacking, Penetration Testing, Target Enumeration and Port Scanning Techniques, Vulnerability Assessment, Network Sniffing, SSL strip, Remote Exploitation, Postexploitation, Windows Exploit Development Basics, Generating shell code, Wireless Hacking, Cracking Process.

References

1. Ethical Hacking and Penetration Testing Guide by Rafay Baloch, CRC Press, Taylor and Francis Group, Reprint, 2019
2. Hacking: The Art of Exploitation by Jon Erickson, No Starch Press, 2nd Edition, 2008.

ICT **** Cloud Security

Abstract

This abstract provides an overview of cloud computing fundamentals and explores key security considerations. It begins by tracing the evolution of cloud computing and detailing its essential characteristics, deployment models (public, private, hybrid, community), and service models (IaaS, PaaS, SaaS). Emphasis is placed on the benefits of cloud computing, including scalability, flexibility, and cost-efficiency, as well as the architecture, virtualization techniques, and the role of cloud data centers. Service Level Agreements (SLAs) and the diverse applications leveraging cloud technology are also discussed. Security challenges in cloud environments are analyzed, covering objectives for information security, requirements for secure cloud software development, and effective policy implementation strategies. The discussion extends to infrastructure security, data protection methods, and privacy issues specific to cloud computing. It addresses threats, vulnerabilities, and risk management practices tailored to cloud deployments. Additional topics include business continuity

planning, disaster recovery strategies, and compliance frameworks essential for both internal policies and regulatory requirements. Standards for cloud security protocols such as SAML, OAuth, OpenID, SSL/TLS are outlined, alongside best practices for encrypting data and managing encryption keys.

References

1. Ronald L. Krutz, Russell Dean Vines, "Cloud Security: A Comprehensive Guide to Secure Cloud Computing", Wiley Publishing, 2010.
2. Tim Mather, SubraKumaraswamy, and ShahedLatif, ” Cloud Security and Privacy", Published by O’Reilly Media, Inc., 2009

ICT **** Malware Analysis and Intrusion Detection

Abstract

Introduction to malware analysis, classification, signature based malware detection and classification, machine learning based techniques, static analysis, dynamic analysis, hybrid analysis, case studies, intrusion detection, rule based techniques, signature based techniques, Machine learning techniques for intrusion detection, intrusion detection in IT networks, case studies.

References

1. Michael Sikorski and Andrew Honig's, Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software, No Starch Press, 1st edition, 2012.
2. Michael Hale Ligh, Steven Adair, Blake Hartstein, and Matthew Richard's, Malware Analyst's Cookbook and DVD: Tools and Techniques for Fighting Malicious Code, Wiley publisher, 1st edition, 2010.
3. Michael Hale Ligh, Andrew Case, Jamie Levy, and AAron Walters, The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory, Wiley publishers, 1st edition, 2014.
4. Rebecca Gurley Bace's, Intrusion Detection Systems, Pearson Education, 1st edition, 2000.
5. Terry Escamilla's, Intrusion Detection: Network Security Beyond the Firewall, Prentice Hall publisher, 1st edition, 2001.

ICT **** Security architecture

Abstract

Overview of key concepts, principles, and the role of security architecture in enterprises; Detailed study of TOGAF, SABSA, and Zachman frameworks and their applications; Techniques for identifying, assessing, and documenting security requirements and risks; Principles and practices for designing secure network, software, and system architectures; Implementation and management of various types of security controls and countermeasures; Integration of security practices into the SDLC, including secure coding and testing; Conducting reviews and audits to ensure security architecture compliance and effectiveness;

Examination of current and emerging trends, such as cloud security, Zero Trust, and IoT security.

References

1. Christopher M. King, Curtis Patton ,Security Architecture: Design, Deployment, and Operations, RSA Press.
2. John Sherwood, Andrew Clark, and David Lynas, Enterprise Security Architecture: A Business-Driven Approach.

ICT **** Secure Network Design

Abstract

Introduction to Network Security, Network Traffic Signatures, Understanding Wireless Security, Defending Against Virus Attacks, Social Engineering, Security Policies, Ongoing Security Management, Physical Security and Disaster Recovery.

References

1. Chuck Easttom , Network Defense and Countermeasures: Principles and Practices, Pearson Education, Inc., Second Edition, 2014
2. Randy Weaver, Dawn Weaver, Dean Farwood, Guide to Network Defense and Countermeasures, Third Edition, Cengage Learning, 2014

ICT **** Identity and Access Management

Abstract

Fundamentals of Cyber Security and IAM Overview, IAM/PAM Tools and Implementation, CyberArk Overview and Architecture, User Access Provisioning and CyberArk Management, Advanced IAM/PAM Operations and Compliance.

References

1. Osmanoglu, E. Identity and access management: Business performance through connected intelligence, 1st edition, 2013
2. Sherwood, J., Clark, A., & Lynas, D., Enterprise security architecture: A business-driven approach, 1st edition, CRC Press, 2005
3. Chapple, M., Stewart, J. M., & Gibson, D. Access control and identity management, 1st edition, Jones & Bartlett Learning, 2013
4. Moyle, E., & Kelley, D. Practical cyber security architecture: A guide to creating and implementing robust designs for cyber security architects, 1st edition, Packt Publishing, 2020

Open Electives [3 0 0 3]

ICT **** Game Theory and Applications

Abstract

Introduction, Mathematical Preliminaries, Non-Cooperative Game Theory: Extensive Form Games, Strategies Form Games, Dominant Strategy Equilibria, Nash Equilibria, Matrix Games, Bayesian Games, Cooperative Game Theory: Two Person Bargaining Problem, Coalition Games, Shapely Values, Mechanism Design: Social Choice Functions, Incentive Compatibility and Revelation Theorem, Auctions

References

1. Y Narahari, Game Theory and Mechanism Design, World Scientific, India, 2015
2. Tim Roughgarden, Twenty Lectures of Algorithmic Game Theory, Cambridge University Press, 2016
3. Dario Bauso, Game Theoy with Engineering Applications, SIAM, Philadelphia, 2016

ICT **** Real Time Systems

Abstract

Introduction to Real Time Systems, Resource management, Commonly used approaches for real time scheduling-static scheduling, priority driven scheduling, RM and DM algorithms, Aperiodic jobs and scheduling, Computation of average response time, Various servers: Deferrable, Sporadic etc. Bandwidth computation, Resource access protocols: various resources access protocols and features, Advantages and drawbacks, Priority ceiling protocols and its use in dynamic priority systems, multiprocessor scheduling, Task assignment and conditions, Faults and fault handling, Redundancy and handling redundancy, Real time communication.

References

1. Jane W.S.Liu, Real Time Systems, Pearson Edition-2006.
2. Philip A Laplante, Real-Time Systems design and analysis (3e),Wiley interscience, 2004
3. Philip A Laplante and Seppo J Ovasaka , Real-Time Systems design and analysis; Tools for the practitioners (4e), IEEE press, 2012

ICT **** IoT Security

Abstract

Introduction to IoT- IoT Overview - Definition and Characteristics of IoT - History and Evolution of IoT, IoT Architecture, IoT Security Fundamentals- Security Requirements and Challenges in IoT - Confidentiality, Integrity, Availability - Unique Security Challenges in IoT, Cryptography for IoT- Symmetric Cryptography - Algorithms: AES, DES - Key Management Challenges, Asymmetric Cryptography - Algorithms: RSA, ECC - Public Key Infrastructure (PKI) in IoT, IoT Network Security- Secure Routing Protocols - Securing Network Layer: RPL, 6LoWPAN - Secure Routing Techniques, Intrusion Detection Systems for IoT - IDS Concepts and Types, IoT Security Frameworks and Standards- IoT Security Standards - ISO/IEC Standards for IoT Security - NIST Guidelines for IoT Security, Regulatory Requirements and Compliance

References

1. B. Russell and D. V. Duren, Practical Internet of Things Security, Packt Publishing Ltd, 2016.
2. S. Misra, M. Maheswaran, and S. Hashmi, Security Challenges and Approaches in Internet of Things, Springer International Publishing, 2017.
3. F. Hu., Security and privacy in Internet of things (IoTs): Models, Algorithms, and Implementations, CRC Press, 2016.