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

Table 1: FIRST SEMESTER

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

Total Credits: 20

Table 2: SECOND SEMESTER

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Type</th>
<th>Course</th>
<th>L-T-P</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td>21SN611</td>
<td>SC</td>
<td>Cyber Forensics and Incident Response</td>
<td>3-0-1</td>
<td>4</td>
</tr>
<tr>
<td>21SN612</td>
<td>SC</td>
<td>Reverse Engineering and Malware Analysis</td>
<td>2-0-2</td>
<td>4</td>
</tr>
<tr>
<td>21RM606</td>
<td>SC</td>
<td>Research Methodology</td>
<td>2-0-0</td>
<td>2</td>
</tr>
<tr>
<td>E</td>
<td></td>
<td>Elective I</td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>E</td>
<td></td>
<td>Elective II</td>
<td></td>
<td>3</td>
</tr>
</tbody>
</table>
### Table 3: THIRD SEMESTER

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Type</th>
<th>Course</th>
<th>L-T-P</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td>E</td>
<td>Elective IV</td>
<td>E</td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>21SN798</td>
<td></td>
<td>Dissertation</td>
<td>P</td>
<td>10</td>
</tr>
</tbody>
</table>

Total Credits: 13

### Table 4: FOURTH SEMESTER

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Type</th>
<th>Course</th>
<th>L-T-P</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td>21SN799</td>
<td></td>
<td>Dissertation</td>
<td>P</td>
<td>16</td>
</tr>
</tbody>
</table>

Total credits 69

### Table 5: LIST OF ELECTIVES

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Type</th>
<th>Course</th>
<th>L-T-P</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td>21SN631</td>
<td>E</td>
<td>Security Operations</td>
<td>3-0-0</td>
<td>3</td>
</tr>
<tr>
<td>Course Code</td>
<td>Type</td>
<td>Course Title</td>
<td>Credits</td>
<td>Term</td>
</tr>
<tr>
<td>------------</td>
<td>------</td>
<td>-------------------------------------------------------</td>
<td>---------</td>
<td>------</td>
</tr>
<tr>
<td>21SN632</td>
<td>E</td>
<td>Cloud and Infrastructure Security</td>
<td>3-0-0</td>
<td>3</td>
</tr>
<tr>
<td>21SN633</td>
<td>E</td>
<td>Cybersecurity Governance</td>
<td>3-0-0</td>
<td>3</td>
</tr>
<tr>
<td>21SN634</td>
<td>E</td>
<td>Machine Learning for Cybersecurity</td>
<td>2-0-1</td>
<td>3</td>
</tr>
<tr>
<td>21SN635</td>
<td>E</td>
<td>Mobile Security and Vulnerability Analysis</td>
<td>2-0-1</td>
<td>3</td>
</tr>
<tr>
<td>21SN636</td>
<td>E</td>
<td>Ethical Hacking</td>
<td>1-0-2</td>
<td>3</td>
</tr>
<tr>
<td>21SN637</td>
<td>E</td>
<td>Vulnerability Analysis and Penetration Testing</td>
<td>0-0-3</td>
<td>3</td>
</tr>
<tr>
<td>21SN638</td>
<td>E</td>
<td>Hardware Security</td>
<td>3-0-0</td>
<td>3</td>
</tr>
<tr>
<td>21SN639</td>
<td>E</td>
<td>Blockchains and Decentralized Applications</td>
<td>2-0-1</td>
<td>3</td>
</tr>
<tr>
<td>21SN640</td>
<td>E</td>
<td>Security of Internet of Things</td>
<td>1-0-2</td>
<td>3</td>
</tr>
<tr>
<td>21SN641</td>
<td>E</td>
<td>Advanced Network Security</td>
<td>3-0-0</td>
<td>3</td>
</tr>
<tr>
<td>21SN642</td>
<td>E</td>
<td>Advanced Cryptography</td>
<td>2-1-0</td>
<td>3</td>
</tr>
<tr>
<td>21SN643</td>
<td>E</td>
<td>Game Theory &amp; Its Applications to Security</td>
<td>3-0-0</td>
<td>3</td>
</tr>
<tr>
<td>21SN644</td>
<td>E</td>
<td>Advanced Android Security &amp; Penetration Testing</td>
<td>1-0-2</td>
<td>3</td>
</tr>
<tr>
<td>21SN645</td>
<td>E</td>
<td>Data Analytics for Security</td>
<td>2-0-1</td>
<td>3</td>
</tr>
<tr>
<td>21SN646</td>
<td>E</td>
<td>SCADA Network Security</td>
<td>3-0-0</td>
<td>3</td>
</tr>
<tr>
<td>21SN647</td>
<td>E</td>
<td>Cyber Law and Privacy</td>
<td></td>
<td>3</td>
</tr>
</tbody>
</table>
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**


TEXTBOOKS / REFERENCES:

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
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  
OSI Security Architecture, security attacks, security services, CIA Triad, Encryption and message confidentiality, symmetric and asymmetric encryption, Message authentication and public key cryptography  
Future directions - Introduction to Cloud Security , Web Security , routing security, wireless security  

TEXTBOOKS/ REFERENCES:  


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 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:


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

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:


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


TEXTBOOKS/ REFERENCES:


5. iPhone and iOS Forensics: Investigation, Analysis and Mobile Security for Apple iPhone, iPad, and iOS Devices by Andrew Hoog, Katie Strzempek 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 & 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:

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:


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

   
   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


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


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


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 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:**


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

Text Books and references


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


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.


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


**TEXT BOOKS/REFERENCES:**
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**

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


Course Objectives


4. HackerOne, “Web hacking 101”
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


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:


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, Demos

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


TEXT BOOKS / REFERENCES:


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)
Module 1

Network Security – Introduction – Overview of Network Attacks


TEXT BOOKS/REFERENCES:


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, bootstrap encryption and Implementation.


**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


TEXT BOOKS/REFERENCES:

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


**TEXTBOOKS / REFERENCES:**


Course Outcomes

CO1: Understanding various data mining techniques for information security (PO3,PSO4)

CO2: 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

TEXT BOOKS / REFERENCES:

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

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:

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:

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


**TEXT BOOKS/REFERENCES:**


**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.


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:


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