M.TECH. CYBER SECURITY SYSTEMS AND NETWORKS

Amrita Center 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 it s application on real-world scenarios. The programme has a strong emphasis on foundational course such mathematics for security application, advanced algorithms, networks etc., 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 the cyber crimes.
3. To be able to architect, design and implement 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.

CURRICULUM

First Semester

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Type</th>
<th>Course</th>
<th>L</th>
<th>T</th>
<th>P</th>
<th>Cr</th>
</tr>
</thead>
<tbody>
<tr>
<td>16MA609</td>
<td>FC</td>
<td>Mathematical Foundations for Cyber Security Systems</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>16SN611</td>
<td>SC</td>
<td>Operating System and Security</td>
<td>3</td>
<td>0</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>16CS602</td>
<td>FC</td>
<td>Advanced Algorithms and Analysis</td>
<td>3</td>
<td>0</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>16SN601</td>
<td>FC</td>
<td>Advanced Computer Networks and Internet Architectures</td>
<td>3</td>
<td>0</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>16SN612</td>
<td>SC</td>
<td>Database and Web Application Security</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>16SN613</td>
<td>SC</td>
<td>Programming Concepts: Practical</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>16HU601</td>
<td>HU</td>
<td>Cultural Education*</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Credits 20

*Non-credit Course
### Second Semester

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Type</th>
<th>Course</th>
<th>L</th>
<th>T</th>
<th>P</th>
<th>Cr</th>
</tr>
</thead>
<tbody>
<tr>
<td>16SN614</td>
<td>SC</td>
<td>Principles of Cryptography</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>16SN602</td>
<td>FC</td>
<td>Cyber Forensics and Incident Response</td>
<td>3</td>
<td>0</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>16SN615</td>
<td>SC</td>
<td>Systems and Network Security - 1</td>
<td>3</td>
<td>0</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>16SN616</td>
<td>SC</td>
<td>Wireless Security</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>E</td>
<td></td>
<td>Elective –I</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>16EN600</td>
<td>HU</td>
<td>Technical Writing*</td>
<td></td>
<td></td>
<td></td>
<td>P/F</td>
</tr>
</tbody>
</table>

Credits 17

*Non-credit course

### Third Semester

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Type</th>
<th>Course</th>
<th>L</th>
<th>T</th>
<th>P</th>
<th>Cr</th>
</tr>
</thead>
<tbody>
<tr>
<td>E</td>
<td></td>
<td>Elective –II</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>E</td>
<td></td>
<td>Elective –III</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>16SN796</td>
<td>P</td>
<td>Live-in-Labs</td>
<td></td>
<td></td>
<td></td>
<td>P/F</td>
</tr>
<tr>
<td>16SN798</td>
<td>P</td>
<td>Dissertation</td>
<td></td>
<td></td>
<td></td>
<td>10</td>
</tr>
</tbody>
</table>

Credits 16

### Fourth Semester

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Type</th>
<th>Course</th>
<th>L</th>
<th>T</th>
<th>P</th>
<th>Cr</th>
</tr>
</thead>
<tbody>
<tr>
<td>16SN799</td>
<td>P</td>
<td>Dissertation</td>
<td></td>
<td></td>
<td></td>
<td>12</td>
</tr>
</tbody>
</table>

Credits 12

**Total Credits: 65**

### List of Courses

#### Foundation Core

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Type</th>
<th>Course</th>
<th>L</th>
<th>T</th>
<th>P</th>
<th>Cr</th>
</tr>
</thead>
<tbody>
<tr>
<td>16MA609</td>
<td>FC</td>
<td>Mathematical Foundations for Cyber Security Systems</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>16CS602</td>
<td>FC</td>
<td>Advanced Algorithms and Analysis</td>
<td>3</td>
<td>0</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>16SN601</td>
<td>FC</td>
<td>Advanced Computer Networks and Internet Architectures</td>
<td>3</td>
<td>0</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>16SN602</td>
<td>FC</td>
<td>Cyber Forensics and Incident Response</td>
<td>3</td>
<td>0</td>
<td>1</td>
<td>4</td>
</tr>
</tbody>
</table>
## Subject Core

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Type</th>
<th>Course</th>
<th>L T P</th>
<th>Cr</th>
</tr>
</thead>
<tbody>
<tr>
<td>16SN611</td>
<td>SC</td>
<td>Operating System and Security</td>
<td>3 0 1</td>
<td>4</td>
</tr>
<tr>
<td>16SN612</td>
<td>SC</td>
<td>Database and Web Application Security</td>
<td>3 0 0</td>
<td>3</td>
</tr>
<tr>
<td>16SN613</td>
<td>SC</td>
<td>Programming Concepts: Practical</td>
<td>0 0 1</td>
<td>1</td>
</tr>
<tr>
<td>16SN614</td>
<td>SC</td>
<td>Principles of Cryptography</td>
<td>3 0 0</td>
<td>3</td>
</tr>
<tr>
<td>16SN615</td>
<td>SC</td>
<td>Systems and Network Security -1</td>
<td>3 0 1</td>
<td>4</td>
</tr>
<tr>
<td>16SN616</td>
<td>SC</td>
<td>Wireless Security</td>
<td>3-0-0</td>
<td>3</td>
</tr>
</tbody>
</table>

## Electives

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course</th>
<th>L T P</th>
<th>Cr</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Elective-I</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16SN700</td>
<td>Distributed Systems and Security</td>
<td>3-0-0</td>
<td>3</td>
</tr>
<tr>
<td>16SN701</td>
<td>Security in the Cloud</td>
<td>3-0-0</td>
<td>3</td>
</tr>
<tr>
<td>16SN702</td>
<td>Formal Methods</td>
<td>3-0-0</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td><strong>Elective-II</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16SN703</td>
<td>Security of Cyber Physical Systems</td>
<td>3-0-0</td>
<td>3</td>
</tr>
<tr>
<td>16SN704</td>
<td>Android Internal Security</td>
<td>2-0-1</td>
<td>3</td>
</tr>
<tr>
<td>16SN705</td>
<td>Principles of Machine Learning</td>
<td>3-0-0</td>
<td>3</td>
</tr>
<tr>
<td>16SN706</td>
<td>Systems and Network Security - 2</td>
<td>3-0-0</td>
<td>3</td>
</tr>
<tr>
<td>16SN707</td>
<td>Mobile Computing and Security</td>
<td>3-0-0</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td><strong>Elective-III</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16SN708</td>
<td>Malware Analysis</td>
<td>2-0-1</td>
<td>3</td>
</tr>
<tr>
<td>16SN709</td>
<td>SCADA Network Security</td>
<td>3-0-0</td>
<td>3</td>
</tr>
<tr>
<td>16SN710</td>
<td>Software Protection</td>
<td>3-0-0</td>
<td>3</td>
</tr>
<tr>
<td>16SN711</td>
<td>Security of Internet of Things</td>
<td>3-0-0</td>
<td>3</td>
</tr>
<tr>
<td>16SN712</td>
<td>Digital Systems Security</td>
<td>3-0-0</td>
<td>3</td>
</tr>
<tr>
<td>16SN713</td>
<td>Binary Exploitation</td>
<td>2-0-1</td>
<td>3</td>
</tr>
</tbody>
</table>

## Project Work

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course</th>
<th>L T P</th>
<th>Cr</th>
</tr>
</thead>
<tbody>
<tr>
<td>16SN798</td>
<td>Dissertation</td>
<td></td>
<td>10</td>
</tr>
<tr>
<td>16SN799</td>
<td>Dissertation</td>
<td></td>
<td>12</td>
</tr>
</tbody>
</table>
Logic, Mathematical reasoning, Sets, Basics of counting, Relations.
Graph Theory: Euler graphs, Hamiltonian paths and circuits, planar graphs, trees, rooted and binary trees, distance and centres in a tree, fundamental circuits and cut sets, graph colorings and applications, chromatic number, chromatic partitioning, chromatic polynomial, matching, vector spaces of a graph.
Analytic Number Theory: Euclid’s lemma, Euclidean algorithm, basic properties of congruences, residue classes and complete residue systems, Euler-Fermat theorem, Lagrange’s theorem and its applications, Chinese remainder theorem, primitive roots.
Algebra: groups, cyclic groups, rings, fields, finite fields and their applications to cryptography.
Linear Algebra: vector spaces and subspaces, linear independence, basis and dimensions, linear transformations and applications.

TEXTBOOKS / REFERENCES:
4. N. Deo, “Graph theory with applications to Engineering and Computer Science”, Prentice Hall of India, New Delhi, 1974.
Covert channels. Introduction to Kernel exploitation - User space vs. Kernel space Attacks, Kernel Stack Vulnerabilities. Case study - Linux kernel, Android, Damn Vulnerable Linux (DVL)

TEXTBOOKS / REFERENCES:


16CS602 ADVANCED ALGORITHMS AND ANALYSIS 3-0-1-4


TEXT BOOKS/ REFERENCES:

16SN601 ADVANCED COMPUTER NETWORKS AND INTERNET ARCHITECTURES 3-0-1-4


Network layer – Internet Addresses, ARP, RARP, IP, Routing algorithm – Interior and Exterior routing, ICMP, Classless and Subnet Address Extensions (CIDR), Internet Multicasting, NAT, VPN – Addressing and Routing, VPN with private address, Internet Security and Firewall design, Transport layer services and principles – Principles of congestion control. Socket Introduction-address structures-Value-Result Arguments, Byte Ordering function, Byte manipulation functions. Elementary TCP sockets. TCP Client/Server Model of Interaction and examples. Denial-of-service (DOS) attacks. Impact of wireless technology on transport protocols. RIP, OSPF, BGP, MPLS


TEXTBOOKS/REFERENCES:


16SN612 DATABASE AND WEB APPLICATION SECURITY 3-0-0-3

Database security – Introduction includes threats, vulnerabilities and breaches, Basics of database design, DB security – concepts, approaches and challenges, types of access controls, Oracle VPD, Discretionary and Mandatory access control – Principles, applications and polymorphisation, Database inference problem, types of inference attacks, distributed database, security levels, SQL-injection: types and advanced concepts, Security in relational data model, concurrency controls and locking, SQL extensions to security (Oracle as an example), System R concepts, Context and control based access control, Hippocratic databases, Database watermarking, Database intrusion, Secure data outsourcing, Web application security, Basic
principles and concepts, Authentication, Authorization, Browser security principles; XSS and CSRF, same origin policies, File security principles, Secure development and deployment methodologies, Web DB principles, OWASP – Top 10 - Detailed treatment, IoT security – OWASP Top 10 – Detailed treatment, Mobile device security – Introduction, attack vector and models, hardware centric security aspects, SMS / MMS vulnerabilities, software centric security aspects, mobile web browser security, Application security – Concepts, CIA Triad, Hexad, types of cyber attacks, Introduction to software development vulnerabilities, code analyzers – Static and dynamic analyzers, Security testing / Penetration testing – Principles and concepts, PT work flows and examples, blind tests, ethical hacking techniques, synthetic transactions, interface testing and fuzzing, SDLC phases and security mandates

TEXTBOOKS/REFERENCES:

16SN613 PROGRAMMING CONCEPTS: PRACTICAL 0-0-1-1


Higher level programming Concepts including Socket Level programming, RPC, High level networking using Java/Python.

TEXTBOOKS/REFERENCES:

16SN614 PRINCIPLES OF CRYPTOGRAPHY 3-0-0-3

Mathematics for cryptography (probability theory, complexity theory, number theory, algebra) Symmetric Key Cryptographic Systems - Caesar and affine ciphers, mono-alphabetic substitutions, transposition, homophonic, Vigenère and Beaufort ciphers, one-time pad, product/iterated/block ciphers, DES and AES.

Cryptanalysis of symmetric key ciphers - attack models, linear, differential and other cryptanalysis techniques, meet-in-the-middle attack. Public (asymmetric) Key Cryptographic Systems (PKCS) - Concepts of PKCS, Diffie-Hellman key-exchange protocol, RSA, Rabin and El Gamal cryptosystems, primality testing, pollard rho factorization

Hash Functions and MACs - Hash functions: the Merkle-Damgard construction, Message Authentication Codes (MACs). Boolean functions - discrete Fourier transform on Boolean functions, Parseval's relation, cryptographic criteria for Boolean functions, nonlinearity, balancedness and resiliency, algebraic immunity, bent Boolean functions.

**TEXTBOOKS/REFERENCES:**


**16SN602 CYBER FORENSICS AND INCIDENT RESPONSE 3-0-1-4**


**TEXTBOOKS/REFERENCES:**


**16SN615 SYSTEMS AND NETWORK SECURITY - 1 3-0-1-4**


TEXT BOOKS/REFERENCES:

16SN616 WIRELESS SECURITY 3-0-0- 3


TEXT BOOKS/REFERENCES:


16EN600 TECHNICAL WRITING P/F (Non-credit Course)


TEXTBOOKS/REFERENCES:


16SN700 DISTRIBUTED SYSTEMS AND SECURITY 3-0-0-3


Fault tolerance: Process resilience, reliable unicast and multicast communication, distributed commit, check pointing and recovery. Security: Threats, policies, mechanisms, secure channels, access control and security management.

Case studies: Enterprise Java Beans, Globe distributed shared objects, NFS/DFS, Amoeba operating system, web server clusters.

TEXTBOOKS/REFERENCES:

1. Andrew S. Tanenbaum and Maarten van Steen, “Distributed Systems: Principles and

TEXT BOOKS / REFERENCES:


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
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

TEXT BOOKS / REFERENCES:


16SN703 SECURITY OF CYBER PHYSICAL SYSTEMS 3-0-0- 3


TEXTBOOKS/ REFERENCES:


16SN704 ANDROID INTERNALS AND SECURITY 2-0-1- 3

TEXT BOOKS/REFERENCES:
4. Adapted Materials from Android development sites.

16SN705 PRINCIPLES OF MACHINE LEARNING 3-0-0-3

Role of learning in intelligent behavior, Designing a learning system; learning from example; Concept learning, Bayesian decision theory, Bayesian Learning, Decision tree learning: Univariate Trees , Classification Trees , Regression Trees, Rule Extraction from Trees, Learning Rules from Data, linear discrimination, SVMs: linear SVMs, introduction to kernel methods, multilayer perceptrons, Local models, Competitive Learning, Incorporating Rule-Based Knowledge, Computational Learning Theory, Instance based Learning, Learning sets of Rules, Analytical Learning, Boosting algorithms, Combining multiple learners, Reinforcement learning.

TEXTBOOKS/ REFERENCES:
Application Security – Introduction – Overview of Attacks Against Applications, Attacking SUID Programs, Environment Attacks, Input Argument Attacks, File Access Attacks, Smashing the Stack for Fun and Profit, Format String Attacks, Assembly Primer, ELF File Format, PLT and GOT, Data and BSS Overflow, Array Overflow, Non-terminated String Overflow, Heap Overflow, Tools and Defenses


TEXT BOOKS/REFERENCES:
4. Larry L.Peterson, Bruce S. Davie, Computer Networks: A Systems Approach

TEXTBOOK AND REFERENCES:

2. This will be a research paper based course. Students are expected to read, summarize and discuss assigned research papers in the field for each class.

16SN708 MALWARE ANALYSIS 2-0-1-3


TEXT BOOKS / REFERENCES:

16SN709 SCADA NETWORK SECURITY 3-0-0-3

Introduction-Critical Infrastructure Control System Cybersecurity Background, Brief History of Critical Infrastructure and ICS, Overview of ICS Processes & Roles Types of ICS Systems, Fundamental principles and concepts of SCADA, DCS, PLCs, Field components, Real-Time Operating systems and Ladder Logic, Communications and OLE for Process Control (OPC), DCS vs. SCADA, IT & ICS Differences, ICS Lifecycle Challenges Physical Security, ICS Network Architecture, Network Models, Design Example, Industrial Control Systems (ICS) characteristics, threats and vulnerabilities, Introduction to PLC and role in

TEXT BOOKS / REFERENCES:

16SN710 SOFTWARE PROTECTION 3-0-0-3

Offensive and Defensive strategies - Offense – Motivation, Methods of attacking software protection. Defense: Methods for hiding information, purpose, algorithms in software.
Program Analysis Static analysis: Control flow analysis, data flow analysis, dependence analysis.
Dynamic analysis: Debugging, tracing, profiling, emulation.
Static Code obfuscation - In-depth Semantics preserving obfuscating transformations, complicating control flow, opaque predicates, data encoding, breaking abstractions.
Obfuscation – Theoretical Bounds Various impossibility results.
Tamper roofing and Watermarking Definitions, Algorithms for Tamperproofing, Remote Tamperproofing.

TEXTBOOKS/REFERENCES:

16SN711 SECURITY OF INTERNET OF THINGS 3-0-0-3


TEXT BOOKS / REFERENCES:

16SN712 DIGITAL SYSTEMS SECURITY 3-0-0-3


TEXT BOOKS / REFERENCES:
Overview – Memory Corruption Attacks, Defenses, ASLR, Bypassing Stack Cookies, DEP, ROP, SROP, Heap Overflow- heap structure, corruption, use after free, C++ differences and concepts, Introduction to kernel exploitation, Kernel vulnerabilities, Kernel memory attacks, Windows kernel overview, Practical windows exploitation, Remote kernel exploitation

Future - Fuzzing, Taint analysis, Dynamic instrumentation

TEXT BOOKS / REFERENCES: