M. Tech. - Computer Engineering
Specialization: Information Security
Curriculum Structure
(w. e. f. 2016-17)

List of Abbreviations

OEC - Institute level Open Elective Course
PSMC – Program Specific Mathematics Course
PCC- Program Core Course
DEC- Department Elective Course
LLC- Liberal Learning (Self learning) Course
MLC- Mandatory Learning Course (Non-credit course)
LC- Laboratory Course
### Semester I

<table>
<thead>
<tr>
<th>Sr. No.</th>
<th>Course Code/Type</th>
<th>Course Name</th>
<th>Teaching Scheme</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>OEC</td>
<td>Security of Information Systems</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>2.</td>
<td>PSMC</td>
<td>Probability, Statistics and Queuing Theory</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>3.</td>
<td>PCC</td>
<td>Foundation of Cryptography</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>4.</td>
<td>PCC</td>
<td>Advanced Operating System</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>5.</td>
<td>PCC</td>
<td>Information Theory and Coding</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>6.</td>
<td>DEC</td>
<td>Elective – I</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>a. System Security Management</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>b. Advancement in Networking</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>c. Machine Learning</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7.</td>
<td>LC</td>
<td>Security Laboratory</td>
<td>--</td>
<td>4</td>
</tr>
<tr>
<td>8.</td>
<td>MLC</td>
<td>Research Methodology</td>
<td>1</td>
<td>--</td>
</tr>
<tr>
<td>9.</td>
<td>MLC</td>
<td>Humanities</td>
<td>1</td>
<td>--</td>
</tr>
</tbody>
</table>

| Total   | 20               | 0             | 6             | 20      |

### Semester II

<table>
<thead>
<tr>
<th>Sr. No.</th>
<th>Course Code/Type</th>
<th>Course Name</th>
<th>Teaching Scheme</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>PCC</td>
<td>Network Security</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>2.</td>
<td>PCC</td>
<td>Applied Cyber Security</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>3.</td>
<td>PCC</td>
<td>Wireless and Mobile Security</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>4.</td>
<td>DEC</td>
<td>Elective – II</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>a. Advanced Database and Information Retrieval</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>b. Cloud Computing and Security</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>c. Software Design Techniques and Security</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.</td>
<td>DEC</td>
<td>Elective – III</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>a. Internet of Things</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>b. Web Technology</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>c. Formal Methods</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.</td>
<td>SLC</td>
<td>MOOC (Massive Open Online Course)</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>7.</td>
<td>LC</td>
<td>Mini Project/Case study</td>
<td>--</td>
<td>4</td>
</tr>
<tr>
<td>8.</td>
<td>MLC</td>
<td>Intellectual Property Rights</td>
<td>1</td>
<td>--</td>
</tr>
<tr>
<td>9.</td>
<td>LLC</td>
<td>Liberal Learning Course</td>
<td>--</td>
<td>1</td>
</tr>
</tbody>
</table>

| Total   | 19               | 0             | 4             | 20      |
### Semester-III

<table>
<thead>
<tr>
<th>Sr. No.</th>
<th>Course Code</th>
<th>Course Name</th>
<th>Teaching Scheme</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Dissertation</td>
<td>Dissertation Phase – I</td>
<td>--</td>
<td>14</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>L</td>
<td>T</td>
</tr>
<tr>
<td>Total</td>
<td></td>
<td></td>
<td>--</td>
<td>--</td>
</tr>
</tbody>
</table>

### Semester-IV

<table>
<thead>
<tr>
<th>Sr. No.</th>
<th>Course Code</th>
<th>Course Name</th>
<th>Teaching Scheme</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Dissertation</td>
<td>Dissertation Phase – II</td>
<td>--</td>
<td>20</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>L</td>
<td>T</td>
</tr>
<tr>
<td>Total</td>
<td></td>
<td></td>
<td>--</td>
<td>--</td>
</tr>
</tbody>
</table>
SEMESTER - I

OEC: Security of Information Systems

Teaching Scheme
Lectures: 3 hrs/week

Examination Scheme
T1, T2 – 20 marks each, End-Sem Exam - 60

Course Outcomes:

1. Analyze functional and non-functional requirements to produce a system architecture that meets those requirements.
2. Use secure medium in Information System.

Unit 1: Introduction (07 hrs)
Define and understand the term information systems (IS). Technology, people, and organizational components of an information system, various types of information systems nature of information systems in the success and failure of modern organizations, understand and plan for the future of managing IS. Information systems for automation, organizational learning and strategic support, Formulate and present the business case for a system

Unit 2: Security in Databases (07 hrs)
Databases, Large Databases, Big Data, Security of this data

Unit 3: E-commerce and their security (07 hrs)

Unit 4: Information Systems Ethics (07 hrs)
Impact of computer ethics on information systems, Issues associated with information privacy, accuracy, property and accessibility.

Unit 5: Computer Crime, and Security

Computer crime and list several types of computer crime, computer virus, worm, Trojan horse, and logic or time bomb, various methods for providing computer security, I T Act 2000

Unit 5: Internet and its security

Use of internet in Information Systems, Security while using internet

Text books:
2. "Introduction to Information Technology", V. Rajaraman, PHI

Reference books:
1. “Information Systems Management in Practice” Barbara C. McNurlin, Ralph H. Sprague, and Publisher: Pearson Education.

(PSMC) Probability, Statistics and Queuing Theory

Teaching Scheme
Lectures: 3 hrs/week

Examination Scheme
T1, T2 – 20 marks each, End-Sem Exam - 60

Course Outcomes:
1. This course will provide necessary understanding in probability, statistics and queuing theory.
2. Solve various problems on probability, statistics and queuing theory.
3. Analyze the given probabilistic model of the problem.
4. Use the techniques studied in probability, statistics and queuing theory to solve problems in domains such as data mining, machine learning, network analysis.

Unit 1: Basic Probability Theory

(3 Hrs)
- Probability axioms, conditional probability, independence of events, Bayes’ rule, Bernoulli trials

Unit 2: Random Variables and Expectation

(10 Hrs)
- Discrete random variables: Random variables and their event spaces, Probability Mass Function, Discrete Distributions such as Binomial, Poisson, Geometric etc., Indicator random variables
- Continuous random variables: Distributions such as Exponential, Erlang, Gamma, Normal etc., Functions of a random variable
- Expectation: Moments, Expectation based on multiple random variables Transform methods, Moments and Transforms of some distributions such as Binomial, Geometric, Poisson, Gamma, Normal

Unit 3: Stochastic Processes

(5 Hrs)
- Introduction and classification of stochastic processes, Bernoulli process, Poisson process, Renewal processes

Unit 4: Markov chains

(8 Hrs)
- Discrete-Time Markov chains: computation of n-step transition probabilities, state classification and limiting probabilities, distribution of time between time changes, M/G/1 queuing system
- Continuous-Time Markov chains: Birth-Death process (M/M/1 and M/M/m queues), Non-birth-death processes, Petri nets

Unit 5: Statistical Inference

(7 Hrs)
- Parameter Estimation – sampling from normal distribution, exponential distribution, estimation related to Markov chains
- Hypothesis testing

Unit 6: Regression and Analysis of Variance

(7 Hrs)
- Least square curve fitting, Linear and non-linear regression, Analysis of variance
Text Books:

References:

PCC: Foundation of Cryptography

Teaching Scheme
Lectures: 3 hrs/week

Examination Scheme
T1, T2 – 20 marks each, End-Sem Exam - 60

Course Outcomes:
1. Understand modern concepts related to cryptography and cryptanalysis
2. Analyze and use methods for cryptography and reflect about limits and applicability of these methods
3. Reason about the details and design philosophy of modern symmetric and public key systems
4. Have a better appreciation of the uses and limitations of the various categories of cryptographic algorithms and understand that great care is needed in their selection and use
5. Reason that security is a systems problem, and that technical methods such as cryptography can only form part of the solution

Unit 1: Introduction (07 hrs)
Unit 2: Number Theory (07 hrs)

Modular Arithmetic, Euclidean Algorithm, Prime Numbers, Relatively Prime Numbers, Primitive Roots, Fermat’s Little Theorem, Euler Totient Function, Extended Euclidean Algorithm, Chinese Remainder Theorem, Discrete Logarithms, Index Calculus Algorithm

Unit 3: Private-key Encryption (07 hrs)

Block Ciphers, Stream Ciphers, Feistel Ciphers, Data Encryption Standard (DES), Cracking DES, Triple DES, Modes of Operation, Advanced Encryption Standard (AES), RC5, International Data Encryption Algorithm (IDEA), cryptanalysis, Weak Keys

Unit 4: Public-key Encryption (07 hrs)


Unit 5: Homomorphic Encryption (07 hrs)


Unit 6: Authentication (07 hrs)


Text books:

Reference Books:

2. Johannes Buchmann, "Introduction to Cryptography", Springer

PCC: Advanced Operating Systems

Teaching Scheme
Lectures: 3 hrs/week

Examination Scheme
T1, T2 – 20 marks each, End-Sem Exam - 60

Course Outcomes:

Students should be able to:

1. Identify and solve problems in distributed, multiprocessor and database operating systems.
2. Explain the architectural features and solutions for implementing various virtualization features in operating systems.
3. Solve synchronization problems involving distributed and virtualized environments.

Unit 1: Distributed Operating Systems (8 Hrs)


Unit 2: Synchronization (06 Hrs)

Clock synchronization, Event ordering, Mutual exclusion, Deadlock, Election algorithms, Desirable features of good global scheduling algorithms, Task assignment approach,
Load balancing approach, Load sharing approach, Process management: Process migration, Threads

Distributed Deadlock Detection, Centralized/Distributed/Hierarchical control, Path Pushing Algorithm, Edge-Chasing Algorithm, Ho-Ramamoorthy Algorithms.

Unit 3: Resource Management in Distributed Systems (06 Hrs)
Distributed File Systems: Mounting, Caching, Bulk Data Transfer, Design Issues, Cache Consistency, Scalability, Log Structured File systems; Distributed Shared Memory: Central-Server Algorithm, Full-Replication Algorithm, etc. Coherence Protocols, Granularity, Page Replacement; Distributed Scheduling: Load, Classification, Load Balancing and Load Sharing, Policies for Transfer, Selection, Location, Information, Stability, Load Balancing Algorithms, Load Sharing Case Studies

Unit 4: Fault Tolerance, Recovery, Protection and Security (06 Hrs)

Unit 5: Multiprocessor and Database Operating Systems (08 Hrs)
Tightly and Loosely Coupled systems, Interconnect networks, Caching, Hypercube architectures, Threads, Process Synchronization in MP systems, Process Scheduling in MP systems, Requirements of Database OS, Transactions, Conflicts, Serializability Theory, Distributed Database Systems, Concurrency control Algorithms, Lock Based Algorithms, Timestamp Based Algorithms, 2PL,

Unit 6: Virtualisation (08 Hrs)
Introduction; Simulation, Emulation, Para-Virtualization, Full virtualization;
**x86 Virtualization:** privileged instructions, control sensitive instructions, Trap and Emulate, Binary translation, x86 hardware virtualization vmxon/vmoff, vmentry, vmexit; Intel VTd, VMCS, Shadow page tables, EPT/NPT

**Text Books:**
3. IA-32/64 Software Developers' Manual Volume 3A, 3B

**References:**

---

**PCC: Information Theory and Coding**

**Teaching Scheme**
Lectures: 3 hrs/week

**Examination Scheme**
T1, T2 – 20 marks each, End-Sem Exam – 60

**Course Outcomes:**
Students will be able to:

1. Gain substantial knowledge of information and entropy, and their use in information theory,
2. Learn principles data compression
3. Understand techniques of design and performance evaluation of error correcting codes
4. Design and develop solutions for technical issues related to information coding
5. Get exposure to emerging topics in information theory, coding and compression.
Unit 1: Introduction to Information Theory (08 Hrs)


Unit 2: Introduction to Coding (08 Hrs)

Classification of codes, Kraft-McMillan inequality, Source coding theorem, Shannon-Fano coding, Huffman coding, Extended Huffman coding, mutual information - Discrete memory less channels – BSC, BEC – Channel capacity, Shannon limit

Unit 3: Source Coding: Text, Audio and Speech (07 Hrs)

Text: Adaptive Huffman Coding, Arithmetic Coding, LZW algorithm – Audio: Perceptual coding, Masking techniques, Psychoacoustic model, MEG Audio layers I,II,III, Dolby AC3 - Speech: Channel Vocoder, Linear Predictive Coding

Unit 4: Source Coding: Image and Video (07 Hrs)


Unit 5: Error Control Coding: Block Codes (06 Hrs)

Definitions and Principles: Hamming weight, Hamming distance, Minimum distance decoding-Single parity codes, Hamming codes, Repetition codes - Linear block codes, Cyclic codes – Syndrome calculation, Encoder and decoder – CRC
Unit 6: Error Control Coding: Convolutional Codes (06 Hrs)

Convolutional codes – code tree, trellis, state diagram - Encoding – Decoding: Sequential search and Viterbi algorithm – Principle of Turbo coding

Text books:

Reference books/paper(s):

Web Resources:
1. NPTEL Course (Information Theory and Coding – IIT, Bombay) : http://nptel.ac.in/syllabus/117101053/
2. MIT OpenCourseWare (Information Theory) : http://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-441-information-theory-spring-2010/index.htm
DEC: System Security Management

Teaching Scheme
Lectures: 3 hrs/week

Examination Scheme
T1, T2 – 20 marks each, End-Sem Exam - 60

Course Outcomes:

1. Evaluate vulnerabilities in the computer systems

2. Learn basic practical security principles and contribute to computer systems and infrastructure

3. Apply methods for authentication, access control, intrusion detection and prevention

4. Employ the security fundamentals to the management aspects of computer system security

Unit 1: Introduction (04 Hrs)

Unit 2: Database Security (05 Hrs)
The Need for Database Security, Database Management Systems, Relational Databases, Database Access Control, Inference, Statistical Databases, Database Encryption

Unit 3: Malicious Software (05 Hrs)
Unit 4: Trusted Computing and Multilevel Security (07 Hrs)


Unit 5: Software Security and Operating System Security (08 Hrs)


Unit 6: Management Issues (10 Hrs)


References:

DEC: Advancement in Networking

Teaching Scheme
Lectures: 3 hrs/week

Examination Scheme
T1, T2 – 20 marks each, End-Sem Exam – 60

Course Outcomes:
Students will be:

1. Capable of implementing various routing protocols
2. To have in depth knowledge of socket programming
3. Aware of issues in SAN, SDN and Open Stack Networking

Unit 1: (06 Hrs)
Routing Protocols: Distance Vector (RIP), Link State (OSPF), Interdomain Routing (BGP), IP Version 6 (IPv6).

Unit 2: (06 Hrs)
Transport Layer Introduction, TCP, UDP, and SCTP

Unit 3: (07 Hrs)
Sockets Introduction, Elementary TCP Sockets, IO Multiplexing, Socket Options, Elementary UDP Sockets, elementary SCTP Sockets

Unit 4: (07 Hrs)
Advanced Sockets, Daemon Processes and the Inetd Superserver, Advanced IO Options, Non blocking I/O

Unit 5: (08 Hrs)
Routing Sockets, Broadcasting, Multicasting, Advanced UDP Sockets, Raw Sockets, Out-of-Band Data, Signal Driven IO, IP Options, Data Link Access
Unit 6: (06 Hrs)

Storage and Networking, Software Defined Networks, Open Stack Networking, Neutron.

TEXT BOOKS:


5. Thomas D'Nadeau and Ken Grey, Software Defined Networking, O'Reilly, 2013


DEC: Machine Learning

Teaching Scheme
Lectures: 3 hrs/week

Examination Scheme
T1, T2 – 20 marks each, End-Sem Exam - 60

Course Outcomes:
Students will be able to:

1. Design hypothesis model for any real-life problem.
2. Apply linear regression, logistic regression and regularization to any machine learning problem.
3. Apply learning techniques like decision trees, Bayesian theory, clustering, SVM, ANN, etc., to solve a real-life problem.
4. Evaluate and perform diagnoses of any machine learning system.
5. Apply learned machine learning techniques to Information security domains

Unit 1: Introduction to Machine Learning (05 Hrs)
Examples of ML Application, Design Perspective and Issues in ML, Supervised, Unsupervised, and Semi-supervised Learning with applications, Concept Learning, Version Space and Candidate-Elimination Algorithm, Inductive Bias

Unit 2: Linear regression, Logistic regression and Regularization (08 Hrs)
Linear regression with one variable: Model representation, cost function, gradient descent
Linear regression with multiple variables: Multiple features, Model representation, cost function, gradient descent: Feature scaling, mean normalization, learning rate
Logistic regression: Classification, hypothesis representation, decision boundary, cost function, gradient descent, advanced optimization, multiclass classification.
Regularization: Problem of over-fitting, cost function, regularized linear regression, regularized logistic regression

Unit 3: Machine learning diagnostic and System design (07 Hrs)
Machine learning diagnostic: debugging a learning algorithm, evaluating a hypothesis [Model selection], training/validating/testing procedures, diagnosing bias versus variance and vice versa, regularization and bias/variance, learning curves
Machine learning system design: Prioritizing what to work on [discuss with case study], error analysis, error metrics for skewed classes, Confusion metric, precision, recall, tradeoff between both, accuracy, datasets for machine learning
Unit 4: Learning Techniques (10 Hrs)

**Bayesian theory:** Bayes rule, probabilistic classifiers, Maximum Likelihood Estimation, case study

**Clustering:** Unsupervised learning technique, k-means algorithm, optimization objective, random initialization, choosing value of k, EM algorithm, Hierarchical clustering

**Decision Tree:** representation, hypothesis, issues in Decision Tree Learning, Pruning, Rule extraction from Tree, Learning rules from Data

**Dimensionality Reduction:** Subset Selection methodologies, Factor Analysis, Multidimensional Scaling

Unit 5: Artificial Neural Networks and Support Vector Machine (06 Hrs)

Non-linear hypothesis, ANN representation, Perception, Training Perception, MLP with BP, Radial Basis Function Network, examples, multi-class classification using ANN Support Vector Machines: Objective [optimization], hypothesis, SVM decision boundary, kernels: RBF and others

Unit 6: Case Studies (04 Hrs)

Profiling the online storefronts of counterfeit merchandise, Detecting malicious web sites in adversarial classification, Credit card fraud detection, Topic models of the underground Internet economy, Learning to rate vulnerabilities and predict exploits

References:

2. Jiawei Han, Jian Pei, Micheline Kamber, Data Mining –Concepts and Techniques, Elsevier, 09-Jun-2011.
3. Ethem Alpaydin, Introduction to Machine Learning, PHI, 2005
4. K.P. Soman, R. Longonathan and V. Vijay, Machine Learning with SVM and Other Kernel Methods, PHI-2009
5. Christopher M. Bishop, Pattern Recognition and Machine Learning, Springer 2006

**LC: Security Laboratory**

**Teaching Scheme**
Practical: 4 hrs/week

**Examination Scheme**
Term Work: 50 marks
Oral Examination: 50 marks

**List of Assignments:**
Students should carry out three assignments each related to topics from the Foundation of Cryptography, Advanced Operating System and Information Theory and Coding courses.
(MLC) Research Methodology

**Teaching Scheme**
Practical: 1 hr/week

**Examination Scheme**
End-Sem Examination: 50 marks

<table>
<thead>
<tr>
<th>Course Outcomes:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Understand research problem formulation</td>
<td></td>
</tr>
<tr>
<td>2. Study various approaches of investigation of solutions for research problems</td>
<td></td>
</tr>
<tr>
<td>3. Learn effective literature survey approaches</td>
<td></td>
</tr>
<tr>
<td>4. Learn ethical practices to be followed in research</td>
<td></td>
</tr>
<tr>
<td>5. Apply research methodology in case studies</td>
<td></td>
</tr>
<tr>
<td>6. Acquire skills required for presentation of research outcomes (report and technical paper writing, presentation etc.)</td>
<td></td>
</tr>
</tbody>
</table>

**Syllabus Contents:**

**Unit 1** (2 Hrs)
Meaning of research problem, Sources of research problem, Criteria Characteristics of a good research problem, Errors in selecting a research problem, Scope and objectives of research problem.

**Unit 2** (3 Hrs)
Approaches of investigation of solutions for research problem, data collection, analysis, interpretation, Necessary instrumentations

**Unit 3** (3 Hrs)
Effective literature studies approaches, analysis

**Unit 4** (2 Hrs)
Plagiarism, Research ethics
Effective technical writing, how to write report, Paper, Developing a Research Proposal, Format of research proposal, a presentation and assessment by a review committee

References:
2. Wayne Goddard and Stuart Melville, “Research Methodology: An Introduction”

(MLC) Humanities

Teaching Scheme
Lectures: 1 hr/week

Examination Scheme
T1, T2 – 20 marks each, End-Sem Exam - 60

Course Outcomes:
1. Understand the development of Civilization, Culture and Social Order over the Centuries
2. Analyze the impact of development of Technology on the Society’s Culture and vice-versa
3. Understand the concept of Globalization and its effects.
4. Compare the positive and negative effects of Industrialization and Urbanization,
5. Appreciate the need of Humanities learning in engineering education

Syllabus Contents:
- **Introduction:** (1 Hr.)
  The meaning of Humanities and its scope. The importance of Humanities in Society in general and for Engineers in particular.
- **Social Science and Development:** (6 Hrs.)
  Development of Human Civilization over the centuries, Society and the place of man in society, Culture and its meaning, Process of social and cultural change in modern India, Development of technology, Industrialization and Urbanization, Impact of development of Science and Technology on culture and civilization Urban Sociology and Industrial Sociology – the meaning of Social Responsibility and
Corporate
Social Responsibility – Engineers’ role in value formation and their effects on society.

- Introduction to Industrial Psychology: (7 Hrs.)
  The inevitability of Social Change and its effects -- Social problems resulting from economic development and social change (e.g. overpopulated cities, no skilled farmers, unemployment, loss of skills due to automation, addictions and abuses, illiteracy, too much cash flow, stressful working schedules, nuclear families etc.) – Job Satisfaction -- The meaning of Motivation and their applications at the workplace (e.g. Maslow’s Hierarchy of Needs, McGregor’s Theory X and Y, The Hawthorne Experiments, etc.) – The need to enrich jobs through skill and versatility enhancement – Ergonomics as a link between Engineering and Psychology

References:
2. Raman Sharma, “Social Changes in India”
4. Ram Ahuja, “Social Problems in India”

SEMESTER – II

PCC: Network Security

Teaching Scheme
Lectures: 3 hrs/week

Examination Scheme
T1, T2 – 20 marks each, End-Sem Exam - 60

Course Outcomes:
1. Understand security issues related to networking vulnerabilities, firewalls, intrusion detection systems
2. Identify infrastructure components including devices, topologies, protocols, systems software, management and security
3. Design and develop solutions for technical issues related to networking and security problems.
4. Apply footprinting, scanning, enumeration and similar techniques to discover network and system vulnerabilities
5. Analyze performance and risk factors of enterprise network systems

Unit 1: Introduction (09 Hrs)
Overview of security in networking, Vulnerabilities in TCP/IP model, IP Attacks, ICMP Attacks, Routing Attacks, TCP Attacks, Application Layer Attacks, Denial of Service attacks (DOS), Distributed DOS, Network threats and protection: Malware, And Spam, Phishing attacks, Remote-Access Trojan, Identifying Network Worms and Viruses, Botnets and Cyber Security

Unit 2: Authentication Mechanisms (07 Hrs)
Authentication Basics, Passwords, Authentication Tokens, Certificate-based authentication, Biometric Authentication, Kerberos, Key Distribution Centres (KDC), Security Handshake Pitfalls, Single Sign On (SSO)

Unit 3: Web Security Protocols (07 Hrs)
Basic concepts, Secure Socket Layer (SSL), Transport Layer Security (TLS), Secure Hyper Text Transfer Protocol (SHTTP), Secure Electronic Transaction (SET), SSL versus SET, 3-D Secure Protocol, Email Security, Pretty Good Privacy (PGP), S/MIME

Unit 4: Digital Certificates and PKI (07 Hrs)
Digital Certificates, Private- Key Management, The PKIX model, Public key Cryptography Standards (PKCS), XML and PKI security, Cross-site Scripting vulnerability

Unit 5: IPSec and VPN (06 Hrs)
IP security overview, Authentication Header, Encapsulating Security Payload, Virtual Private Network (VPN), IPSec verses VPN, Network Address Translation (NAT), Secure Routing, Secure Multicast
Unit 6: Firewalls and IDS (06 Hrs)

Firewall basics, Demilitarized zone, typical firewall configuration, Firewall types, Intrusion Detection systems, Detection verses Prevention, types of IDS, Intrusion Prevention Systems (IPS), Honeypots

Text books:
2. Charlie Kaufman, Radia Perlman and Mike speciner, “Network security, Private communication in a Public World”
4. V. K. Pachghare “Cryptography and Information Security”, PHI

Reference books:

Web Resources:
1. http://nptel.iitm.ac.in/courses/106105031/
7. http://www.cs.northwestern.edu/~ychen/classes/cs395-w05/lectures.html
   http://www.cs.iit.edu/~cs549/cs549s07/lectures.htm
PCC: Applied Cyber Security

Teaching Scheme
Lectures: 3 hrs/week

Examination Scheme
T1, T2 – 20 marks each, End-Sem Exam – 60

Course Outcomes:

1. Explore the legal, ethical, and global impact of cybercrime on private, public, and personal computing infrastructures

2. Collect, process, analyse, and present computer forensic evidence

3. Demonstrate an Understanding of network forensics

4. Develop an understanding of the legal issues associated with cyber security

5. Understand the core concepts, tools, and methods used to secure computer systems.

Unit 1: Introduction (06 Hrs)

Unit 2: Cyber Crime Issues (07 Hrs)
Unauthorized Access to Computers, Computer Intrusions, white collar Crimes, Viruses and Malicious Code Internet Hacking and Cracking, Virus Attacks

Unit 3: Privacy and Cyber Law (07 Hrs)
Software Piracy, Pornography, Intellectual Property, Mail Bombs, Exploitation, Stalking and Obscenity in Internet, Digital laws and legislation, Law Enforcement Roles and Responses

Unit 4: Cyber Crime (07 Hrs)
Unit 5: Investigation (06 Hrs)

E-Mail: Investigation, Tracking and E-Mail Recovery, IP Tracking, Case Studies. Encryption and Decryption Methods, Search and Seizure of Computers, Deleted Evidences recovery, Password Cracking

Unit 6: Digital Forensics (07 Hrs)


Text books:


Reference books:


PCC: Wireless and Mobile Security

Teaching Scheme
Lectures: 3 hrs/week

 Examination Scheme
T1, T2 – 20 marks each, End-Sem Exam - 60

Course Outcomes:

1. Gain knowledge on security and privacy topics in wireless and mobile networking
2. Understand the security and privacy problems in the realm of wireless networks and
mobile computing

3. Apply proactive and defensive measures to counter potential threats, attacks and intrusions

4. Analyze the various categories of threats, vulnerabilities, countermeasures in the area of wireless and mobile networking

5. Design secured wireless and mobile networks that optimize accessibility whilst minimizing vulnerability to security risks

6. Research in the field of mobile and wireless security and privacy

**Unit 1: Introduction**  
(08 Hrs)

Introduction to wireless networks security: Wired vs. wireless network security, Threat categories and the OSI model, Vulnerabilities, Countermeasures, Security architectures. IEEE 802.11 standard security issues: Authentication and authorization mechanisms, Confidentiality and Integrity, pre-RSNA protocols (WEP), RSNA (802.11i), Key management, Threat analysis and case studies. Mobile networks security

**Unit 2: Mobile Security**  
(06 Hrs)

Mobile system architectures, Overview of mobile cellular systems, GSM and UMTS Security architecture & Attacks, Vulnerabilities in Cellular Services, Cellular Jamming, Attacks & Mitigation, Security in Cellular VoIP Services, Mobile application security.

**Unit 3: Securing Wireless Networks**  
(06 Hrs)

Overview of Wireless security, Scanning and Enumerating 802.11 Networks, Attacking 802.11 Networks, Attacking WPA protected 802.11 Networks, Bluetooth Scanning and Reconnaissance, Bluetooth Eavesdropping, Attacking and Exploiting, Bluetooth, Zigbee Security, Zigbee Attacks

**Unit 4: Ad-hoc Network Security**  
(07 Hrs)

Unit 5: RFID Security (08 Hrs)

Unit 6: Mobile Commerce Security (06 Hrs)
Reputation and Trust, Intrusion Detection, Vulnerabilities, Analysis of Mobile commerce platform, secure authentication for mobile users, Mobile commerce security, payment methods, Mobile Coalition key evolving Digital Signature scheme for wireless mobile Networks

Text Book:

Reference Books:

DEC: Advanced Database and Information Retrieval

Teaching Scheme Examination Scheme
Lectures: 3 hrs/week T1, T2 – 20 marks each, End-Sem Exam - 60

Course Outcomes:

1. Understand foundation of RDBMS theory, internal functioning of a typical RDBMS
2. Design and implement algorithms for various relational operators such as join, group by etc.
3. Analyze and understand latest trends of RDBMS.
4. Understand and discuss current issues and research in searching and information retrieval
5. Understand and analyze Query Language and Operation with respect to IR.
6. Analyze evaluation techniques and apply the IR concepts to digital library

Unit 1: Transaction Processing (07 hrs)

Unit 2: Query Processing and Optimization (07 hrs)
Architecture of Query Execution Engines, Disk Access, Aggregation and Duplicate Removal, Sorting and Hashing, Binary Matching Operations (Join Algorithms), Execution of complex query plans, Nested Relations, Additional Techniques for performance improvement, Query Evaluation Techniques for Large Databases, Basic Query Optimization.

Unit 3: Latest Trends in Databases (07 hrs)
Study of Hadoop Distributed File System; HIVE - Data warehousing application built on top of Hadoop, MapReduce-It is a patented software framework introduced by Google in 2004 to support distributed computing on large data sets on clusters of computers; Dynamo – It is a highly available, proprietary key-value structured storage system or a distributed data store; Eventual Consistency Model for Distributed Systems.

Unit 4: IR Modeling (07 hrs)
Data Retrieval Vs Information Retrieval, Goals and history of IR, The impact of the web on IR, The role of AI in IR, Applications of IR, Basic Models of IR: Boolean and vector-space retrieval models, ranked retrieval, weighting, cosine similarity.

Unit 5: Query Languages and Operations (06 hrs)
Keyword-Based Querying, Pattern Matching, User Relevance Feedback, Automatic Local Analysis, Automatic Global Analysis

Unit 6: Retrieval Evaluation and Digital Library (06 hrs)

Text books:

Reference books:


DEC: Cloud Computing and Security

Teaching Scheme
Lectures: 3 hrs/week

Examination Scheme
T1, T2 – 20 marks each, End-Sem Exam - 60

Course Outcomes:
1. Characterize the distinctions between various cloud models and services
2. Compare the functioning and performance of virtualization of CPU, memory and I/O with traditional systems
3. Familiar with OpenStack components and other cloud platforms to create a cloud infrastructure and services
4. Analyze the security risks associated with cloud computing and evaluate how to address them
Unit 1: Introduction (06 Hrs)

Benefits and challenges to Cloud architecture, Cloud delivery models - SaaS, PaaS, LaaS.
Cloud Deployment Models - Public Cloud, Private Cloud, External Cloud and Hybrid Cloud, Service level agreements in clouds, case studies on Cloud services: Azure, Google App Engine, Amazon Web Services

Unit 2: Virtualization (08 Hrs)

Virtualization: Role of virtualization in enabling the cloud, Levels of Virtualizations, Types of Virtualization: Compute, Network and Storage Virtualizations, Virtual Machine, Hypervisor: Type 1 and 2
Server Virtualization: X86 architecture, Protected mode, Rings of Privileges, Virtualization challenges, Full virtualization and Binary Translation, ESXi, Para-Virtualization, Xen, Hardware Assisted Virtualization, System call and hardware interrupts handling in virtualized systems, Intel VTx, KVM, VM Migration

Unit 3: Memory and I/O Virtualization (10 Hrs)

Memory management and I/O with traditional OS, Challenges in virtualized system, Shadow page Tables in Full Virtualized system, EPT/NPT, 2D Page walks, I/O in Virtualized Systems, Emulation, Split drivers of Xen, Direct I/O, Intel VTd, VTc, VMCS

Unit 4: Virtualization Security (06 Hrs)

Security Challenges Raised by Virtualization, Virtualization Attacks, VM Migration Attacks, Launch Pad for Brute Force attacks, Security Solutions, Hypervisor-Based Segmentation, case studies of Hypervisors

Unit 5: Cloud Orchestration (06 Hrs)

Elements of Cloud Orchestration, Examples platforms: OpenStack and vSphere
**OpenStack Deep dive:** Covers Networking, Storage, Authentication modules of OpenStack, Nova, Quantum, Keystone and Cinder, Swift

**VSphere:** Architecture, vCenter, Distributed Services, VMFS, Memory Optimization Techniques of ESX

**Unit 6: Cloud Security**

SaaS security issues, Attack on Data Availability, PaaS security issues, Rogue Clouds, Lack of Auditability, Security Solutions, Law Enforcement, Security as a Service, case studies

**References:**

2. Dinakar Sitaram and Geetha Manjunath, Moving to the cloud, Elsevier
3. V.K. Pachghare, Cloud Computing, PHI

**On-line Course Resources:**

1. Understanding Full Virtualization, Para Virtualization and Hardware Assist, VMware White paper
2. AMD-V Nested Paging, white paper, July 2008
5. "OpenStack Docs: Current", http://docs.openstack.org/

**DEC: Software Design Techniques and Security**

<table>
<thead>
<tr>
<th>Teaching Scheme</th>
<th>Examination Scheme</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lectures: 3 hrs/week</td>
<td>T1, T2 – 20 marks each, End-Sem Exam - 60</td>
</tr>
</tbody>
</table>

**Course Outcomes:**

1. Explore the legal, ethical, and global impact on software design by considering security as an inbuilt feature.
2. Collect, process, analyze, and implement different models by making use of security principles and properties.
3. Demonstrate an understanding of software design techniques from a security perspective.
4. Develop an understanding of the legal issues associated with security.
5. Understand the core concepts, tools, and methods used to design secure systems.

**Unit 1:** (06 Hrs)


**Unit 2:** (06 Hrs)
Requirements Engineering for secure software: Introduction, the SQUARE process Model, Requirements elicitation and prioritization

Unit 3: (08 Hrs)
Secure Software Architecture and Design: Introduction, software security practices for architecture and design: architectural risk analysis, software security and reliability knowledge for architecture and design: security principles, security guidelines and attack patterns

Unit 4: (07 Hrs)
Secure coding and Testing: Code analysis, Software Security testing, Security testing considerations throughout the SDLC, white-box testing, black-box testing, and penetration testing and secure coding.

Unit 5: (07 Hrs)
Security and Complexity: System Assembly Challenges: introduction, security failures, functional and attacker perspectives for security analysis, system complexity drivers and security

Unit 6: (06 Hrs)
Governance and Managing for More Secure Software: Governance and security, Adopting an enterprise software security framework, How much security is enough?, Security and project management, Maturity of Practice.

TEXT BOOK:


REFERENCE BOOKS:

1. Developing Secure Software: Jason Grembi, Cengage Learning
5. Fundamentals of Software Engineering, Rajib Mall, PHI, 2005
7. Software Engineering1: Abstraction and modeling, Diner Bjorner, Springer
8. Software Engineering2: Specification of systems and languages, Diner Bjorner,
10. Software Engineering 3: Domains, Requirements and Software Design, D.Bjorner,
11. Software Engineering Principles and Practice, Hans Van Vliet, 3 edition, Wiley India
    edition.
12. Introduction to Software Engineering, R.J.Leach, CRC Press.
    University Press, 2009

DEC: Internet of Things

Teaching Scheme
Lectures: 3 hrs/week

Examination Scheme
T1, T2 – 20 marks each, End-Sem Exam - 60
Course Outcomes:

1. Identify and design the new models for market strategic interaction
2. Analyze various protocols for IoT
3. Design a middleware for IoT
4. Analyze and design different models for network dynamics

Unit 1: Introduction (08 Hrs)

Introduction to IoT: - Definition and Characteristics.

Web of Things V/s Internet of Things: - Two pillars of the web, architecture standardization for WoT, Platform middleware for IoT, Unified multitier WoT architecture, WoT portals and Business Intelligence.

M2M to IoT: M2M Communication, Trends in Information and Communication Technology, Implications for IoT, Barrier and Concern for IoT.

Unit 2: (08 Hrs)

IoT Architecture: Building architecture, Main design principles and needed capabilities, An IoT architectural overview.


IoT Reference Architecture: Deployment and Operational view.

Unit 3: (06 Hrs)

M2M and IoT Technology Fundamentals: Gateway, Local and wide area networking, Managing IoT, Data consideration for M2M data, M2M and IoT analytics, Knowledge Management.

Recent Protocol for IoT: Power line Communication, IPv6 over Low Power WPAN, Routing protocol for low Power and lossy network RPL, ZigBee Smart energy 2.0, ESP8266 M2M architecture, MQ telemetry transport
Unit 4: (06 Hrs)

**OS Requirement of IoT Environment:** RiOT, mbed, Contiki, typical components of an OS for low end IoT devices.

**Recent Protocol for IoT:** Power line Communication, IPv6 over Low Power WPAN, Routing protocol for low Power and lossy network RPL, ZigBee Smart energy 2.0, ESPI M2M architecture, MQ telemetry transport.

Unit 5: (06 Hrs)

**Security for IoT:** Security Issues, Challenges, Spectrum of security consideration, privacy consideration, Interoperability Issues, Regularity, Legal and Right Issues, A policy based framework for security and Privacy in IOT

Unit 6: (06 Hrs)

**IoT Smart Application:** Agriculture, Smart cities, Smart Energy and Smart Grid, Smart Mobility and Transport, Smart Homes, Smart Building and Infrastructure, Smart Health etc.

**Case Studies:** Leading tools manufacturer transform operation with IoT (CISCO), Market Disputation and Improved Customer Relationship, Internal transformation for IoT business model Reshapes connected Industrial Vehicle.

**TEXT BOOKS:**

1. Internet of Things: Converging Technologies for smart Environments and Integrated Ecosystems, Dr. Ovidiu Vermesan, Dr. Peter Friess, River Publication.

**REFERENCES:**
2. Designing the Internet of Things, Adrian McEwen, Hakim Cassimally.
6. Operating System for low end devices in IOT: Survey, Oliver Hahm, Emmanuel Baccelli, Hauke Petersen, Nicolas Tsiftes, Dec 2015, HAL-hal-01245551.

DEC: WEB SYSTEMS AND TECHNOLOGIES

Teaching Scheme
Lectures: 3 hrs/week

Examination Scheme
T1, T2 – 20 marks each, End-Sem Exam – 60

Course Outcomes:

1. Understand the fundamental of web protocols.
2. Learning different web related technologies currently used.
3. Studying data handling in web systems.
4. Analyzes the nature of web and application level security and describes how to solve problems on a practical basis.
5. Analyzing wide range of web security vulnerabilities and issues.

Unit 1: Web Essentials (06 Hrs)

Unit 2: Introduction to Client-Side Programming (07 Hrs)
Introduction to JavaScript, Basic Syntax, Variables and Data Types, Statements, Operators, literals, functions. JavaScript Objects–properties, references, methods, constructors, Arrays, other built-in objects, Debugging JavaScript, Introduction to Host Objects, Document Object Model (DOM), Document tree, DOM event handling, jquery, YUI Library

Unit 3: Server-Side Programming (06 Hrs)
Java servlet: architecture, life cycle. The Client Request – form data, request headers. The Server Response– HTTP Status Codes, HTTP Response Headers. Sessions, Cookies, URL Rewriting, Concurrency in servlets, Separating Programming and Presentation: Java server pages, Basic JSP, JavaBeans Classes and JSP, JSF, Java Database Connectivity (JDBC), PHP

Unit 4: Representing Web Data (07 Hrs)
XML–Namespaces, AJAX–Overview, basics, toolkits, security, DOM based XML processing, XSL, XPath, XSLT, Content Management Frameworks (Drupal, Joomla, etc.)

Unit 5: Application Security (08 Hrs)
Injection Attacks
SQL Injection Attacks ,Blind Injection, Timing Attack ,Database Attacking Techniques, Common Attack Techniques ,Command Execution, Stored Procedure Attacks, Coding Problems, SQL Column Truncation, Properly Defending against SQL Injection, Using Precompiled Statements, Using Stored Procedures, Checking the Data Type ,Using Safety Functions ,Other Injection Attacks ,XML Injection ,Code Injection, CRLF Injection,

Authentication and Session Management
Who Am I?, Password ,Multifactor Authentication ,Session Management and Authentication ,Session Fixation Attacks, Session Keep Attack ,Single Sign-On
Unit 6: Web configuration security (06 Hrs)


Text Books:


References:


On-line Course Resources:

1. https://www.youtube.com/playlist?list=PL04D5787E247DC324
2. https://drive.google.com/file/d/0BxCZDgp07VbHBl3Z5T1JQd00/edit?pli=1
3. http://www.w3schools.com/
6. https://www.drupal.org/node/877140

DEC: Formal Methods

Teaching Scheme
Lectures: 3 hrs/week

Examination Scheme
T1, T2 – 20 marks each, End-Sem Exam – 60

Course Outcomes:

1. Describe the mathematical foundation of Formal Methods
2. Analyse case studies for architecting the formal models
3. Compare various formal models and its coverage of state transition system
4. Design experimental setup to verify for the given case studies
5. Design Specification and verification expressions for software systems

Unit 1: Introduction (06 Hrs)
Genealogy of Formal Verification: Early Beginnings of Mathematical Logic, Automated Theorem Proving, Beginning of Program Verification, Dynamic Logic and Fixpoint Caluli, Temporal Logic, Decidable Theories and ω-Automata

Unit 2: A Unified Specification Language (07 Hrs)

Unit 3: Fixpoint Caluli (07 Hrs)
Partial Orders, Lattices and Fixpoint, The Basic \( \mu \)-Calculus, Monotonicity of State Transformers, Model Checking of the Basic \( \mu \)-Calculus: A Naïve Model Checking Procedure, Optimization by the Alternation Depth

Unit 4: Finite Automata (07 Hrs)
Regular Languages, Regular Expressions and Automata, The Logic of Automata Formulas, Boolean Closure, Converting Automata Classes, Determinization and Complementation, The Hierarchy of \( \omega \)-Automata and Borel Hierarchy, Automata and Monoids, Decision Procedures for \( \omega \)-Automata

Unit 5: Temporal Logics (07 Hrs)
Introduction to Temporal Logics, Branching Time Logics, Translating Temporal Logics to the \( \mu \)-Calculus, Translating Temporal Logics to the \( \omega \)-Automata, Completeness and Expressiveness of Temporal Logic, Complexities of the Model Checking Problems, Reduction by Simulation and Bisimulation Relation

**Unit 6: Binary Decision Diagrams**

Basic Definitions, Basic Algorithms on BDDs, Minimization of BDDs using Care sets, Computing Successors and Predecessors, Variable Reordering

**Reference books:**


**SCL: MOOC (Massive Open Online Course)**

**Teaching Scheme**

Lectures: 3 hrs/week

**Examination Scheme**

T1, T2 – 20 marks each, End-Sem Exam - 60

**Course Outcomes:**

1. Learn how to search effectively and use the wealth of information freely available on Internet judiciously
2. Imbibe the habit of self learning
3. Get exposure to learning from world class professors
4. Course specific outcomes

**Syllabus Contents:**
Students will be given a list of courses with video lectures delivered by renowned professors available. Based on the response, 1 or 2 courses will be officially finalized and a regular faculty member will be assigned to the selected course(s). The assigned faculty member(s) will address queries of students related to the video lectures and will also be responsible for evaluation of the students just like any other regular subject by conducting quizzes and end-semester examination as per the academic calendar.

**LC: Mini Project/Case study**

1. Mini project is a regular course to conduct and implement/simulate.
2. Student along with PG faculty would decide upon the topic to prepare a plan for project work.
3. Student should get the approval of the Course Coordinator before the first month of the semester when the course is registered.
4. Course duration will be entire semester.
5. Student should submit Project report before completion of the course.
6. Performance of student will be evaluated by committee via mid-term and final evaluation (including external examiner).
7. Mini-Project can be performed individually or maximum group of 2 students.

**MLC: Intellectual Property Rights**

**Teaching Scheme**
Lectures: 3 hrs/week

**Examination Scheme**
T1, T2 – 20 marks each, End-Sem Exam - 60

**Course Outcomes:**

1. Understand that today's world is controlled by Computer, Information Technology, but tomorrow world will be ruled by ideas, concept, and creativity.

2. Understand that IPR would take such important place in growth of individuals and nation. It is needless to emphasize the need of information about Intellectual Property Right to be promoted among students in general & engineering in particular.

3. Understand that IPR protection provides an incentive to inventors for further research work and investment in R & D, which leads to creation of new and better
products, and in turn brings about, economic growth and social benefits.

UNIT 1  (6 Hrs)

UNIT 2  (4 hrs)

UNIT 3  (4 Hrs)

UNIT 4  (4 hrs)
New Developments in IPR: Administration of Patent System. New developments in IPR; IPR of Biological Systems, Computer Softwares etc. Traditional knowledge Case Studies, IPR and IITs

UNIT 5  (4 hrs)
Registered and unregistered trademarks, design, concept, idea patenting.

References:


**SEMESTER - III**

**Dissertation Phase – I**

**Course Outcomes:**

1. Learn how the available literature can be searched for gathering information about a problem/domain

2. Understand the current status of the technology/research in the selected domain

3. Understand software engineering principles related to requirements gathering and analysis

4. Understand how to evaluate different design techniques and methods to find out the best feasible solution under given constraints for the given problem

5. Understand how to write requirements analysis and design documents

The dissertation / project topic should be selected / chosen to ensure the satisfaction of the urgent need to establish a direct link between education, national development and productivity and thus reduce the gap between the world of work and the world of study.

The dissertation should have the following:

i. Relevance to social needs of society

ii. Relevance to value addition to existing facilities in the institute

iii. Relevance to industry need

iv. Problems of national importance

v. Research and development in various domain

The student should complete the following:

1. Literature survey

2. Problem Definition
3. Motivation for study and Objectives
4. Preliminary design / feasibility / modular approaches

SEMESTER - IV

Dissertation Phase – II

Course Outcomes:
1. Understand software engineering principles related to implementation and testing of software solutions
2. Get a glimpse of how large software are implemented, tested and maintained
3. Understand how to document a large software for making it comprehensible and maintainable
4. Understand how effective testing is an important aspect of software development
5. Understand how to present the work done in various forms (technical report/paper/presentation) at various platforms (conferences/journals/defense of the dissertation etc)

The student should complete the following:
1. Implementation of the proposed approach in the first stage
2. Testing and verification of the implemented solution
3. Writing of a report and presentation
4. (Not mandatory but desired) Publish the work done at suitable conference/in a journal