Model Course Structure/Syllabus
for
M. Tech (IS/ CS with Specialization in IS),
M. Tech/MS by Research,
B. Tech / M. Tech (Retrofit)
6 months / 1 – Yr PG Diploma courses of CDAC / NIELIT

Ministry of Electronics & Information Technology
Electronics Niketan
6 CGO Complex
Lodhi Road, New Delhi – 110003
Preface

After the successful completion of ISEA Project Phase I, Government of India approved ISEA Project Phase II, which involves participation of large number of academic institutions viz. IITs, NITs, IIITs, Technical Universities, autonomous societies of MeitY, etc. selected at different levels and offering various courses in Information Security. The Academic and Research Advisory Committee (ARAC) set up under the project; Chaired by Prof N Balakrishnan had set up a sub-committee: Syllabus Revision Committee with Prof Sukumar Nandi-IIT Guwahati, Prof V Kamakoti-IIT Madras, Prof Alwyn Pais-NIT Surathkal and Prof M S Gaur-MNIT Jaipur (Member Convenor). Further, a sub-committee: an Expert Committee was set up under the Chairmanship of Prof. N Balakrishnan along with Prof R K Shyamasundar-IIT Bombay, Prof C E Veni Madhavan-IISc. Bangalore, Shri Sanjay Kumar Vyas-MeitY and Shri Ch A S Murty-CDAC Hyderabad to review the draft course structure/syllabus.

At the outset, the ARAC recommended a methodology to be adopted for Syllabus Revision. Accordingly, Syllabus Revision Committee discussed the issues/trends/research opportunities/industry requirements, etc. and finalized the approach for syllabus revision and started with the model syllabus prescribed under ISEA Project Phase I. The Committee also compiled current syllabi offered in various IITs, NITs and discussed the gaps/emerging areas suitable for revising the syllabus. The scope of draft structure/syllabi revision includes both, formal and non-formal courses such as MS by Research/ M. Tech by Research, specialized M. Tech programs viz. M. Tech (IS) & M. Tech (CS with IS), Retrofitting of Information Security courses at M. Tech / B. Tech level and two diploma courses of CDAC & NIELIT.

The purpose of this exercise is to design a model course structure/syllabus, which act as a benchmark for various formal and non formal course being offered under the project. In this document, emphasis has been given on core fundamental subjects along with various specialized subjects/electives in different streams such as Cryptography, Infrastructure and Communication, Secure Programming, Database applications, Information Security Management, etc. As a result, the total number of courses suggested under these streams has increased to 55 from erstwhile 29 courses suggested in previous ISEA project. Each course is thoroughly reviewed by experts in the field of Information Security. Each institution is free to choose any combination of the courses from the streams depending upon their specializations and academic competence. While appropriate books and references are prescribed, course instructors may refer/adopt additional references / text books, if required.

The Committee faced several challenges in designing the course structure/syllabus but with continuous support of mentors, faculty members, MeitY & ISEA PMU, this exercise has been completed.

At the end, we must thank Prof N Balakrishnan for his continuous guidance, support and critical technical inputs; Syllabus Revision Committee members Prof Sukumar Nandi, Prof V Kamakoti and Prof Alwyn Pais for drafting syllabus; and faculty members of Department of CSE, MNIT Jaipur for contributing in this immense task. This could not have been achieved without the active support and critical technical inputs of Expert Committee members namely Prof C E Veni Madhavan, Prof R K Shyamasundar and Shri Sanjay Kumar Vyas. We also acknowledge the efforts put up in by ISEA-PMU team particularly by Shri Ch A S Murty, Shri K S Balaji and Shri Chandan Sharma in collecting and collating details of various courses being taught in the reputed international universities and colleges from across the globe.

Member Convenor
Syllabus Revision Committee
ISEA Project Phase II
Acknowledgements

Expert Committee for Syllabus Revision

i. Prof. N Balakrishnan, IISc. Bangalore – Chairman
ii. Prof. C E Veni Madhavan, IISc. Bangalore
iii. Prof. R K Shyamasundar, IIT Bombay
iv. Shri. Sanjay Kumar Vyas, MeitY
v. Shri. Ch. A S Murty, C-DAC Hyderabad

Syllabus Revision Committee

i. Prof. Sukumar Nandi, IIT Guwahati
ii. Prof. V Kamakoti, IIT Madras
iii. Prof. Alwyn Pais, NIT Surathkal
iv. Prof. M S Gaur, MNIT Jaipur – Member Convener

Others

i. ISEA-PMU
Structure of the course

M Tech (Information Security)

- 10 courses + one major project + internship may be offered M. Tech (IS) program, with the following break up:
  - Minimum of four to five courses from core module – (20 – 25% in terms of credits)
  - Minimum of three courses from one of the relevant streams viz. cryptography, infrastructure & communication models, information security management, data analytics, secure programming, cyber-crime & forensics
  - Minimum three elective courses from any other stream/s besides previously chosen stream

The details of the core module, specialized courses, and electives courses are at Annexure I
Credit models of Information Security courses are at Annexure II
The detailed syllabus of Core and Specialized courses are at Annexure III

- Major project (carrying one third weightage in terms of credits) focusing on any topic from relevant stream chosen by a candidate aimed at demonstrating the concept, research, design, implementation or analysis.
- Internship with industry (3-6 months) will gives an opportunity to gain industrial experience & develop an understanding of what they have learned relates to real world issues and to put into practice the techniques taught to them.

Pre-requisites

- Four Year Bachelor’s degree in Electronics, IT, Computer Science, Communication Engineering, or equivalent or any other stream with at-least two courses in the IT and Programming.

M Tech (Computer Science with specialization in Information Security)

- 6 courses + one major project + internship [Optional] may be offered M. Tech (CS with specialization on IS) program, with the following break up:
  - Minimum of three courses from core module
  - Minimum of three courses from one of the relevant streams viz. cryptography, infrastructure & communication models, information security management, data analytics, secure programming, cyber-crime & forensics

The details of the core module, different streams, & relevant courses are at Annexure I
Credit models of Information Security courses are at Annexure II
The detailed syllabus of Core and Specialized courses are at Annexure III

- Major project (carrying one third weightage in terms of credits) focusing on any topic from relevant stream chosen by a candidate aimed at demonstrating the concept, research, design, implementation or analysis.
- Internship with industry (3-6 months) [Optional] will gives an opportunity to gain industrial experience & develop an understanding of what they have learned relates to real world issues and to put into practice the techniques taught to them.

Note: The above are broad guidelines only. Each Institute/Technical University may follow a different pattern and there is a complete flexibility in adapting to the basic requirements / structure appropriately.

Note: The criteria mentioned above are suggestive only. Each Institute/Technical University may also follow pre-existing norms of their institute
- Some of the institute are considering MCA / M. Sc (Mathematics (with at least 2 courses in the Computer Science Courses) / Computer Science / IT) may also be consider to be eligible.)
Pre-requisites

- Four Year Bachelor’s degree in Electronics, IT, Computer Science, Communication Engineering, or equivalent or any other stream with at-least two courses in the IT and Programming

Note: The above are broad guidelines only. Each Institute/Technical University may follow a different pattern and there is a complete flexibility in adapting to the basic requirements / structure appropriately

Note: The criteria mentioned above are suggestive only. Each Institute/Technical University may also follow pre-existing norms of their institute
- Some of the institute are considering MCA / M. Sc (Mathematics (with 2 compulsory courses in the Computer Science Courses) / Computer Science / IT) may also be consider to be eligible

M. Tech / B. Tech (Retrofit)

- For M. Tech retrofitting, any 2 – 3 courses from the core module on Information Security should offer from the list of core / specialized courses and electives mentioned in the Annexure I. In addition to it, dissertation on Information Security research area may be considered.
- For B. Tech retrofitting, any 2 – 3 courses from the core module on Information Security at 5th Semester onwards may be adopted through retrofitting in the existing scheme in department / open electives. Also, the final year project work may also include a module on Information Security.

The details of the core module, specialized courses, and electives courses are at Annexure I
Credit models of Information Security courses are at Annexure II
The detailed syllabus of Core and Specialized courses are at Annexure III

Note: Any 2 – 3 courses ---> any 2-3 courses from the core module (Flexibility may be given to institutes to offer retrofitted courses depending upon their capabilities)
Proposed M. Tech (CS/IS-Research) Scheme

This scheme is drawn from existing program run by various CFTIs. The course credits are earned from the courses offered in regular M. Tech program. The name is suggested as M. Tech (Research).

Curriculum and Requirements of the M. Tech (Research) Programme in Computer Science and Engineering-IS

- **Duration**
  The general duration of the M Tech (Research) programme is 4 semesters for full-time students. The maximum extensions can be to 6 semesters (8 semesters) for full-time students under special circumstances.

- **Credit Requirements**
  - Total credits : 60
  - Course credits : 20
  - Thesis credits : 40
  - CGPA Requirements
    - Minimum CGPA requirement for award of degree: ‘x’ (As per institute norms)
    - Minimum CGPA in course work for continuation of registration: ‘x’

- **Regulations for registration**
  - *First semester:*
    - Full time students to register for 15-20 course credits only
  - *Later semesters:*
    - Students to register for remaining courses and thesis credits
    - There are no core course requirements (other than the thesis)
    - All Post-Graduate level courses of the CSE/CSE-IS Department are available to the student for course credits. Courses offered by other departments may be taken for credit on the advice and approval of the programme coordinator / thesis supervisor.
    - Student will register for courses on the advice and approval of the M. Tech (Research) programme coordinator (first semester) and the thesis supervisor (subsequent semesters).

- **Supervision**
  - Maximum 2 thesis supervisors. DREC (same as PhD) to assign thesis supervisor within 2 months of registration in Semester 1.
  - DREC will monitor thesis work, based on written reports and presentations made every semester and will recommend number of thesis credits considered as cleared at the end of the semester.
    - X grade will be awarded for continuing thesis research.

- **Evaluation and Examiners**
  - Submission of synopsis one month before submission of thesis. Pre-synopsis seminar to DREC
  - Dean AA to appoint external examiner on receipt of title and synopsis of thesis, from a panel of 4 experts recommended by supervisor and approved by DREC
  - Examination board = thesis supervisor(s) and external expert examiner

- **Thesis Grading**
  - Thesis Defense Committee = External expert examiner (from India and outside Institute), supervisor(s) and DREC.
  - Assistantships On par with M Tech students provided under the project.

- **Conversion to PhD**
  - On application by the student and on recommendation by the DREC. A minimum CGPA of 8.5 after first 2 semesters is required. Student must satisfy other requirements for admission into PhD programme. The date of conversion is the date of registration in the PhD program

*****
### Indicative list of Core, Specialized / Elective subjects & Research / Project Topics

<table>
<thead>
<tr>
<th>Core subjects</th>
<th>Stream</th>
<th>Specialized subjects</th>
<th>Research/Project Topics</th>
</tr>
</thead>
<tbody>
<tr>
<td>IS1. Network Security</td>
<td>Cryptographic Research / Methodologies</td>
<td>ISC1. Topics in Cryptography</td>
<td>• Applied Cryptography</td>
</tr>
<tr>
<td>IS2. Fundamentals of Information Security</td>
<td></td>
<td>ISC2. Applied Cryptography</td>
<td>• Lattice based Cryptography</td>
</tr>
<tr>
<td>IS4. Algorithms &amp; Computational Complexity</td>
<td></td>
<td>ISC4. Game Theory &amp; its Applications</td>
<td>• Symmetric / Asymmetric Encryption algorithms</td>
</tr>
<tr>
<td>IS5. Random Process &amp; Probability</td>
<td></td>
<td>ISC5. Side-Channel Attacks</td>
<td>• Cipher</td>
</tr>
<tr>
<td>IS7. Cryptography</td>
<td></td>
<td>ISC7. Privacy Engineering</td>
<td></td>
</tr>
<tr>
<td>IS10. Advanced Distributed Systems</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IS11. Information Theory &amp; Coding</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IS12. Information Security and Secure Coding</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Information Security Management</td>
<td>ISM1. Information Security Risk Management</td>
<td>• Routing Protocols</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ISM2. PKI &amp; Trust Management</td>
<td>• Wireless Networks</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ISM3. Cyber Law &amp; Rights in Digital Age</td>
<td>• Cognitive Radio</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ISM4. Computer Security Audit and Assurance</td>
<td>• Secure Communications</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ISM5. Strategic Computing and Communication Technologies</td>
<td>• Security and Trustworthiness of Infrastructure</td>
</tr>
<tr>
<td></td>
<td>Network and Data Security Analysis</td>
<td>ISA1. Protocol Analysis</td>
<td>• Critical Infrastructures</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ISA2. Digital Watermarking and Steganalysis</td>
<td>• SCADA Infrastructure Security</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ISA3. Distributed System</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ISA4. Simulation &amp; Modeling</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ISA5. Optimization Techniques</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ISA6. Web Architecture Security</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ISA7. Advanced Distributed System</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ISA8. IoT and its Security</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ISA9. SCADA Security</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ISA10. Advanced Networks</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ISA11. Next Generation Networks</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ISA12. Mobile Computing</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ISA13.IoT and its Security</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ISA14. Platform Based Security</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ISA15. Advanced Networks</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ISA17. Network Security</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ISA19. Introduction to Computer and Networking</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ISA20. Security and Trustworthiness of Infrastructure</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ISA21. SCADA Infrastructure Security</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ISA22. Big Data Analytics</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ISA23. Data Mining</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ISA24. Data Optimization</td>
<td></td>
</tr>
<tr>
<td>Core subjects</td>
<td>Stream</td>
<td>Specialized subjects</td>
<td>Research/Project Topics</td>
</tr>
<tr>
<td>---------------</td>
<td>--------</td>
<td>----------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td></td>
<td>ISA3.</td>
<td>Data Mining and Machine Learning</td>
<td>• Malware Analysis</td>
</tr>
<tr>
<td></td>
<td>ISA4.</td>
<td>Privacy &amp; Security for online Social Networks</td>
<td>• Social Network</td>
</tr>
<tr>
<td></td>
<td>ISA5.</td>
<td>Decision Support System Methods</td>
<td>• Life Data Analysis</td>
</tr>
<tr>
<td></td>
<td>ISA6.</td>
<td>Malware Analysis</td>
<td>• Application Data Analysis</td>
</tr>
<tr>
<td>Cybercrime Investigation and Forensics</td>
<td>ISF1.</td>
<td>Cyber Crime and Information warfare</td>
<td>• Digital Forensics</td>
</tr>
<tr>
<td></td>
<td>ISF2.</td>
<td>Computer Crime Investigation and Cyber Forensics</td>
<td>• Information Forensics</td>
</tr>
<tr>
<td></td>
<td>ISF3.</td>
<td>Cyber Law and rights in the Digital Age</td>
<td>• Cybercrime Detection</td>
</tr>
<tr>
<td></td>
<td>ISF4.</td>
<td>Advanced Forensics</td>
<td>• Cyber ethics</td>
</tr>
<tr>
<td>Cybercrime Investigation and Forensics</td>
<td>ISF5.</td>
<td>Incident Response and Cyber Forensics</td>
<td>• Secure and Privacy</td>
</tr>
</tbody>
</table>

*****
## Credit models of Information Security courses

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Core Course</th>
<th>L – T – P</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td>IS1</td>
<td>Network Security</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IS2</td>
<td>Fundamentals of Information Security</td>
<td>3 – 0 – 0</td>
<td></td>
</tr>
<tr>
<td>IS3</td>
<td>Principles of Data and System Security</td>
<td>3 – 1 – 0</td>
<td></td>
</tr>
<tr>
<td>IS4</td>
<td>Algorithms &amp; Computational Complexity</td>
<td>3 – 0 – 0</td>
<td></td>
</tr>
<tr>
<td>IS5</td>
<td>Random Process &amp; Probability</td>
<td>3 – 0 – 0</td>
<td></td>
</tr>
<tr>
<td>IS6</td>
<td>Programming Abstractions</td>
<td>3 – 0 – 0</td>
<td></td>
</tr>
<tr>
<td>IS7</td>
<td>Cryptography</td>
<td>3 – 0 – 0</td>
<td></td>
</tr>
<tr>
<td>IS8</td>
<td>Wireless Security</td>
<td>3 – 0 – 1</td>
<td></td>
</tr>
<tr>
<td>IS9</td>
<td>Secure System Engineering</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IS10</td>
<td>Advanced Distributed Systems</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IS11</td>
<td>Information Theory &amp; Coding</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IS12</td>
<td>Information Security and Secure Coding</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IS13</td>
<td>Mathematical Foundations for Cybersecurity</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Specialized Courses and Electives</th>
<th>L – T – P</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISC-X</td>
<td>Cryptographic / Research Methodologies</td>
<td>3 – 0 – 2</td>
<td></td>
</tr>
<tr>
<td>ISI-X</td>
<td>Infrastructure and Communication Model</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISM-X</td>
<td>Infrastructure and Security Management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISP-X</td>
<td>Secure Programming</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISA-X</td>
<td>Data Analytics</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISF-X</td>
<td>Cybercrime Investigation and Forensics</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Thesis / Project</th>
<th>L – T – P</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td>--</td>
<td>Project / Dissertation</td>
<td>0 – 0 – 6</td>
<td></td>
</tr>
</tbody>
</table>

*****
Annexure III

Syllabus for Core / Additional Courses to be offered under ISEA Project Phase II

Core Modules – Suggestive Course Codes (ISEA-MT- ISX)

IS1: Network Security

Review and Fundamentals:
- Overview of networking security; Security Services (Confidentiality, Authentication, Integrity, Non-repudiation, access Control and Availability) and Mechanisms; Security Attacks ( Interruption, Interception, Modification and Fabrication)
- Principle of least privilege, access control, and operating systems security
- Authentication overview; Authentication protocols,
- Conventional encryption Principles, algorithms and tools
  - Basics of cryptography: cryptographic hash functions, symmetric and public-key encryption, public key cryptography principles & algorithms, cipher block modes of operation,
  - Secure Hash Functions and HMAC.
- Security Attacks
  - Buffer overflow attacks & format string vulnerabilities,
  - Denial-of-Service Attacks
  - Hijacking attacks: exploits and defenses
  - Internet worms, viruses, spyware, phishing, botnets,
  - TCP session hijacking, ARP attacks, route table modification, UDP hijacking, and man-in-the-middle attacks.
- IP Security Overview & Architecture,
  - Network defense tools: Firewalls, VPNs, Intrusion Detection, and filters
  - Email privacy: Pretty Good Privacy (PGP) and S/MIME.
  - Network security protocols in practice. Introduction to Wireshark. SSL, IPsec, and IKE.
- DNS security
- Web Security Requirements,
  - Secure Socket Layer (SSL) and Transport Layer Security (TLS), Secure Electronic Transaction (SET).

References:
2. Hack Proofing your network by Ryan Russell, Dan Kaminsky, Rain Forest Puppy, Joe Grand, David Ahmad, Hal Flynn Ido Dubrawsky, Steve W.Manzuik and Ryan Perneh, Wiley Dreamtech

IS2: Fundamental Concepts of Information Security

- Information Classification – Guidelines, Types, Criteria for data Classification, Data Classification procedures, Classification Controls
Ethics – Basic Concepts, Professional code of Ethics, Common Computer Ethics Fallacies (responsible disclosure), (cross reference SP/Professional Ethics / Accountability, responsibility and liability), Hacking and Hacktivism

References:
3. Enterprise Information Security and Privacy; By C. Warren Axelrod, Jennifer L. Bayuk, Daniel Schutzer, Artech House Press

**IS3: Principles of Data and System Security**

**Prerequisites:** Discrete Structures, basics of Operating Systems, programming expertise

**Concepts of Security**
Confidentiality, Containment, isolation, Privacy, Anonymity, psuedo- anonymity etc., Policy specification, User authentication, Session management, multi-level security, multi-lateral security

**Security Mechanisms**
Protection, Confinement, Isolation, Virtual machines, Non-interference Dealing with legacy code, Sandboxes, Separability, , Data caging

**Access Control**
Mandatory Access Control, Discrete Access Control, Principles of Least Privilege, Distributed Access Control , Role based Access, Attribute Based Access, Key Management, SPKI/SDSI

**Security Models for Information Systems**
Bell la Padua, Biba, Clark-Wilson, Lattice Model, Chinese Wall Model

**Information Flow Models**
Distributed Information Control, Secure OS based on IFC, Conference management systems like EasyChair, HotCrp…

**OS Security:** Principles, Case studies of Operating Systems, secure OS like SELINUX

**Information Flow Models**
Distributed Information Control (DIFC), Conference management systems EasyChair, HotCrp, certification of programs

**Run-Time Monitoring**
Security Automata, Edit Automata, Shallow Automata

**Malware analysis and Counter measures**
difficulties, approaches, defense against untrusted code

Web security models, application security, Browser Security, Information flow browsers

**Special Topics:** Mobile phone security, Android Security, Cloud security, Security of Internet of Things (IoT)

**Text Books and Resources:**
1. Cryptography and Data Security, Dorothy Denning, Addison Wesley
2. Introduction to Computer Security, Matt Bishop, Pearson Education Publishers
IS4: Algorithms and Computational Complexity

Computational Complexity: Polynomial time and its justification, Nontrivial examples of polynomial-time algorithms, the concept of reduction (reducibility), Class P Class NP and NP- Completeness, The P versus NP problem and why it’s hard
Algorithmic paradigms: Dynamic Programming, Greedy, Branch-and-bound, Divide and Conquer
Randomized Algorithms: Finger Printing, Pattern Matching, Graph Problems, Algebraic Methods, Probabilistic Primality Testing, De-Randomization
Advanced Algorithms:, Graph Algorithms: Shortest paths, Flow networks, Spanning Trees; Approximation algorithms, Randomized algorithms.
Approximation algorithms: Polynomial Time Approximation Schemes.
Advanced Data Structures and applications: Decision Trees and Circuits, B-Trees, AVL Trees, Red and Black trees, Dictionaries and tries, Maps, Binomial Heaps, Fibonacci Heaps, Disjoint sets, Union by Rank and Path Compression

References:

IS5: Random Processes and Probability

Probability Theorem: Properties of probability, Conditional probability, Independence Bayes theorem
Discrete Distributions: Probability distribution functions and cumulative distribution functions
Continuous Distributions: Probability density functions and cumulative distribution functions, joint and marginal probability density functions
Mean and variance; moment -generating functions, Marginal and conditional probability distributions, some specific discrete distributions
Functions of Random Variables: Distribution function technique, Transformation techniques, Moment-generating function techniques
Randomness, Adversaries and Physical World: The Power of probabilistic algorithms, pseudorandom number generators, Zero knowledge proofs

References:
“To be adopted by the course instructor”

IS6: Programming Abstractions

Data abstractions: Elementary and structured data types, their specifications, representations, and implementation of numbers, vectors and arrays, records, character string, variable size data structure, sets, input output files. Type checking and type conversion, type equivalence
Scope and referencing: Scope and Lifetime of Variables, Recursion, Storage management – static, stack, dynamic, fixed/variable size heap; Pointers and Dynamic Memory Allocation
Control abstractions: Implicit and explicit sequence control Subprogram sequence control, Recursive sub programs, Built-in and User-defined Functions, parameters and their transmission, Co-Routines and Scheduled Subprograms, Task and Concurrent exception
Object-Oriented Abstractions: Objects and Classes, Encapsulation, Polymorphism, Inheritance. Aspect Oriented Programming, Introduction to Aspects - Crosscutting concerns, Aspect, Join point and Point cuts
Classical and modern ciphers; pseudorandomness; statistical properties of random sequences; discrete probability; Symmetric key and public key cryptosystems; general design principles of block ciphers; substitution-permutation networks; general design principles of stream ciphers; linear feedback shift-register sequences; boolean functions; canonical examples - DES, 3DES, AES, RC4, RC5, RC6, A5/1,2; Analysis methodologies - differential, linear, square, algebraic techniques. Public key cryptosystems: elementary number theory, abstract algebra, and linear algebra; Diffie Hellman key exchange, public key encryption, digital signatures, Knapsack, RSA, ElGamal, Rabin schemes; Functionalities of entity, content authentication; message digests and hashing schemes; cryptographic embedding in different layers of network stack; applications, protocols and standards; social, economic and geo-political issues

References:

There are many standard, popular, accessible books that cover most of the above material at varying depths of exposition.


Some of these are by - Abhijit Das and Veni Madhavan;

IS8: Wireless Network Security

Overview of Wireless LAN physical components
Wireless LAN topologies and technologies - 802.11 a/b/g/n/ac Features
Understanding, Building and Configuring Wireless Networks
Configure and install wireless adapters, access points, bridges and antennas
Security Features of 802.11 Wireless
WEP, WPA1 and WPA2
PSK Authentication, TKIP Encryption and AES-CCMP Encryption
Security threats and vulnerabilities in Wireless networks
Vulnerabilities of IEEE.11 Security
MAC Address Filtering Weaknesses
hacking Personal Wireless Security, WEP, WPA1 and WPA2
Caffe Latte Attack Basics, Caffe Latte Attack Demo, Koreks Chopchop Attack, Fragmentation And Hirte Attack, Cracking PEAP
Hotspot Attacks, Hacking Isolated Clients

References:

1. 802.11 Wireless Networks: The Definitive Guide by Matthew Gast, O'Reilly Media
2. Next Generation Wireless LANs: 802.11n and 802.11ac by Eldad Perahia and Robert Stacey, Cambridge University Press
3. Controller-Based Wireless LAN Fundamentals: An end-to-end reference guide to design, deploy, manage, and secure 802.11 wireless networks by Jeff Smith, Jake Woodhams, Robert Marg, Cisco press

IS9: Secure Systems Engineering

Unit 1 – Hardware Security
Hardware Trojans and Detection – PUFs - Power Analysis Attacks and Countermeasures - Fault Attacks - Implementation Aspects of Crypto Algorithms (A case study of AES and ECC)

Unit 2 – Micro Architectural Security
Timing attacks and Covert Channels - RAM based attacks - Cold boot - Rowhammer

Unit 3 – Operating System Security

Unit 4 – Application Security
SQL Insertion - Shell Shock - Heart bleed bug

Unit 5 – Formal Verification of Security Protocols

Text Books

5. Aleph One, Smashing the Stack for Fun and Profit, http://insecure.org/stf/smashstack.html

Practicals (4 hours per week * 12 weeks)

Power Analysis Attacks
Given power traces of an encryption system such as AES, the participants would need to build algorithms to determine the secret key.

Fault Attacks
Given a faulty and a fault free ciphertext, the participants would need to write code to determine the secret key.

Timing Attacks
In this assignment, participants would develop a timing attack on encryption systems like the RSA or/and AES.

Stack Smashing Attacks
The intent of this assignment is to understand stack smashing and how they can be used to develop malicious software.

Operating System Side Channels
Demonstrate an OS side channel attack. For instance, using memory footprints to determine the web page browsed.

Other potential lab experiments: PUF design, an ECC crypto-system development, format string vulnerabilities.

Video Lectures:

1. Cryptography: https://www.youtube.com/playlist?list=PLvifRcqO0wF9yDamC0XtD503fA085X6mP
2. IT Security: https://www.youtube.com/playlist?list=PLvifRcqO0wF-AWyoq03Cgg3N0yklA9CjeR
**IS10: Advanced Distributed System**

Shared Memory: Introduction - bus based multi processors ring based multiprocessors switched multiprocessors - NUMA comparison of shared memory systems - consistency models - page based distributed shared memory - shared variable distributed shared memory - object based distributed shared memory. Case studies: MACH and CHORUS

**References:**

**IS11: Information theory and Coding**

Overview; Basic Concepts - Entropy and Mutual information; Lossless Source Coding - Source entropy rate; Kraft inequality; Huffman code; Asymptotic equipartition property; Universal coding; Noisy Channel Coding - Channel capacity; Random channel codes; Noisy channel coding theorem for discrete memoryless channels; Typical sequences; Error exponents; Feedback; Continuous and Gaussian channels; Lossy Source Coding - Rate- Distortion functions; Random source codes; Joint source-channel coding and the separation theorem.
Compression as a Case Study (LZ & MPEG)

**References:**

**IS12: Information Security and Secure Coding**

Unit 1 - (8 Hours) Information Security Basics
Unit 2 - (16 Hours) Information Security Policy and Compliance
Unit 3 - (16 Hours) Secure Application
Secure application design – Writing Secure Software – J2EE vulnerabilities.
Unit 4 - (8 Hours) Secure Infrastructure Management

**Text Books**
1. Name: Information Security – The complete reference; Chapters: 1-9, 11-12, 26-28, 31, 32, and 34

**Practical’s (4 hours per week * 12 weeks)**
Demonstration of attacks after determining vulnerability using hacking tools. Methods to fix such vulnerability to be demonstrated during the practical using the techniques discussed in the book “The CERT C Coding Standard”. Tools to be used from https://www.kali.org/ and freely downloadable vulnerability tools.

Outside class (4 hours per week * 12 weeks)

Reference Book:

Video Lectures:
1. http://nptel.ac.in/courses/106106129/ - Week 1 – Part 1 to 16.
2. Dr. Daniel Soper lectures: https://www.youtube.com/playlist?list=PLlYw7XsK0HV-r0T5fypBv9-a1gbq8xkZR (Parts 1 - 12)

IS13: Math Foundation for Information Security

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.

Probability and Statistics: Introduction to probability concepts, random variables, probability distributions (continuous and discrete), Bayesian approach to distributions, mean and variance of a distribution, joint probability distributions, theory of estimation, Bayesian methods of estimation.

Random Processes: General concepts, power spectrum, discrete-time processes, random walks and other applications, Markov chains, transition probabilities.

Textbooks / References:
4. N. Deo, “Graph theory with applications to Engineering and Computer Science”, Prentice Hall of India, New Delhi, 1974.

******
ISC1: Cryptography - Theory and Practice

The same content as above (Basic Cryptography) with more in-depth coverage on theoretical aspects, algorithms & computations and cryptanalysis.
Some additional topics would be: analytic number theory; group theory; elliptic curves; probabilistic methods in combinatorial analysis; computational complexity; arithmetical and algebraic algorithms; integer factoring- group order, quadratic congruence methods; discrete logarithms- index calculus; algebraic cryptanalysis for block and stream ciphers; one-way functions; hard-core predicates; hash collisions; emerging areas - identity, attribute based encryption; homomorphic encryption; block chains; end-to-end encryption; side-channel attacks and resistance; security engineering; post-quantum crypto algorithms based on hard primitives;

References:

There are many standard, popular, accessible books that cover most of the above material at varying depths of exposition.
Some of these are by - Menezes et al; Koblitz; Abhijit Das and Veni Madhavan;

ISC2: Applied Cryptography

Perfect Ciphers, Symmetric Encryption, Key Exchange, Asymmetric Encryption, Public Key Protocols, Using Cryptographic Primitives, Secure Computation

References:


ISC3: Quantum Cryptography

Quantum computing models, quantum algorithms, quantum tree search, quantum wavelets, quantum information theory, quantum cryptography, breaking RSA system, quantum teleportation, circuit design, quantum error correction

Finite Dimensional Hilbert Spaces – Tensor Products and Operators on Hilbert Space – Hermitian and Trace Operators - Basic Quantum Mechanics necessary for the course.
Quantum Gates and operators and Measurement: Quantum Computational Model – Quantum Complexity – Schemes for Physical realization (Only peripheral treatment expected)
Shor's Algorithm – Application to Integer Factorization – Grover's Algorithm – Quantum Cryptography: Encryption and decryption schemes

References:


ISC4: Game Theory & Its Applications

Game Theory and Its Application: Basics of game theory; Different types of games: two party, multi party games, coalition games ongraphs; Nash equilibrium; Walsarian and other equilibria, Analysis of optimal strategies; Applications of game theory (network economics, bandwidth allocations, etc.)

References:

“To be adopted by the course instructor”
ISC5: Side Channel Attacks
   To be announced later

ISC6: Advanced System Security
   Language Based Security
      Application Information Flow Models; Declassification Requirements
   Database Security
   Privacy Preservation and Compliance
      Compositionality; Access Control Requirements
   Security of Operating Systems
      Centralized Systems; Decentralized Systems
   VM Security
   Cloud Security
      Map reduce security; Hadoop, HDFS etc., Science of Security

Resources:
   Mostly research papers and chapters from different books

ISC7: Privacy Engineering
   To be announced later

ISC8: Analysis and Verification of Cryptographic protocols
   While cryptographic protocols form the backbone of our digital society, the security of various critical components has been neglected. As a result, attacks have lead to catastrophic losses of property and loss of privacy. Developing a secure cryptographic protocol is game-like in nature, and a good designer will consider attacks against key components. The aim of the course is to highlight the secure design of cryptographic protocols and facilitate the evaluation of existing schemes. The course highlights recent advances in formal methods, game theory etc in the specification, analysis and verification of crypticographic protocols with an emphasis on algorithmic analysis. The topics include electronic voting protocols, user-controlled anonymity for direct anonymous attestation, and algorithmic evaluation of observational equivalence. discovering, and fixing, a vulnerability in the RSA-based Direct Anonymous Attestation protocol.

Resources:
   Books on Model Checking, Game Theory and Research Papers on crypto-protocols

ISC9: Specialized courses in Cryptography
   Some of the topics in Cryptography Theory and Practice, in addition to it, as provable security notions; key agreement; secure channels; random oracle assumptions; pseudo-randomness; authenticated encryption; signature protocols; protocol verification

References:
   Research literature from various crypto conferences such as Crypto, Eurocrypt, Asiacrypt, Indocrypt, Latincrypt and journals on cryptology
   *****
Stream: Infrastructure and Communication Models - Suggestive Course Codes (ISEA-MT- ISIX)

ISI1: Introduction to Computer Security

Introduction to techniques for defending against hostile adversaries in modern computer systems and computer networks


Introduction to Network Access Control and Cloud Security- Network Access Controls, Introduction to protocols like SSL, TSL, SSH, IPSEC, Network attacks like denial-of-service (DoS), Distributed Denial Service of Attacks (DDoS) attacks and their defences; Characteristics of Firewalls, IDS, IPS, Intrusion detection; techniques to provide privacy in Internet applications; and protecting digital content (music, video, software) from unintended use.

Malicious Software: Introduction, Types of Malicious Software, propagation of viruses, worms, SPAM, Trojans, System Corruption, Payloads, exploits

Introduction to Operating system security: Underlying Principles of Security Architecture; Physical Security; File Systems Security; Authentication, Authorization and Accountancy

References:
3. Enterprise Information Security and Privacy; By C. Warren Axelrod, Jennifer L. Bayuk, Daniel Schutzer, Artech House Press


Threats of viruses, worms, malicious codes, etc., models of propagation and their epidemic spread, DoS & DDoS attacks and defense, Design of scalable testbeds for simulation of attacks against critical infrastructures, Ubiquitous, Dependable and Indestructible storage.

Analysis techniques disassembly and debugging techniques

Model based risk analysis for critical Infrastructure; Physical Vulnerability assessment; Modelling and simulation tools for CI; Graphic formalism for modelling and Simulation; Semantic interoperability among federated simulators of CI; Game Theory in IS; Cyber security in SCADA Systems; Modelling and measuring and managing Information Technology risks; Trustworthiness evaluation of CI; Network resilience; Monitoring and Surveillance Technology

References:
“To be adopted by the course instructor”

ISI3: Cloud Computing Security


References:

**ISI4: Platform Based Security**

IoT Security, Code integrity and code signing, Secure boot, measured boot, and root of trust Attestation, TPM and secure co-processors, Security threats from peripherals, e.g., DMA, IOMMU, Physical attacks: hardware Trojans, memory probes, cold boot attacks
Security of embedded devices, e.g., medical devices, cars
Trusted path

**References:**

“To be adopted by the course instructor”

**ISI5: Advanced Networks**

The Design Philosophy of the DARPA Internet Protocols, End-to-End Arguments in System Design, Flow Rate Fairness, Overlay and P2P Networking
TCP: Congestion Avoidance and Control, Rate Guarantees, Delay Guarantees.
Software Defined Networking: Network function virtualisation, programmable forwarding planes, Mining as simulation framework for SDN

**References:**


**ISI6: Next Generation Networks**

Overview of limitations of current Internet architecture and Content-Centric Networking as an alternative paradigm;
Content-Centric Networking (CCN) as an architecture replacement for the current IP-based host-centric Internet infrastructure. Named-Data Networking (NDN) as a case for CCN.
Access and Backhaul Networks: Roadmap for NextGen Communication Networks; Wide Area Ubiquitous Network; Wireline Access Networks; Fibre-wireless networks; Wireless Network - LTE; VoLTE

**References:**

“To be adopted by the course instructor”

**ISI7: Mobile Computing**

Introduction to mobile computing: principles, classification & overview of devices, operating systems.
Android Overview, Android Development Environment, Android Studio, Projects, Gradle, Manifest, Resources, Emulators
Anatomy of an App, App Lifecycle, Location of GPS, maps and Google maps, sensing, Gesture, 2D graphics, Drawable, Persistence / Storing Data / Preferences
Network and Web Services of Mobiles- Content Resolvers / Content Providers, Accessing the Calendar and Contacts Providers, Bluetooth, Notifications, Google Play Services
Introduction to Mobile Security – Case study on Android

References:

“To be adopted by the course instructor”

**ISI8: IoT and its security**

**Introduction of IoT**

**Domains of IoT**

**M2M vs IoT**

M2M to IoT; M2M to IoT - A Market Perspective; M2M to IoT - An Architectural Overview; M2M and IoT Technology Fundamentals
Management of IoT

**IoT Communication Protocols**

NFC, RFID, Zigbee; MIPI, M-PHY; UniPro, SPMI, SPI, M-PCIe; Wired vs. Wireless communication, GSM, CDMA, LTE, GPRS, small cell; Vulnerabilities and Risks associated with Protocols

**IoT Platforms**

Hardware, SoC, sensors, device drivers, IoT standards; Cloud computing for IoT; Bluetooth, Bluetooth Low Energy, beacons
Community Impact of IoT: Federal, State, and Local Municipalities

**Security and Privacy Risks, Implications of IoT on various systems:** Brand Damage, Loss of Trust, Intellectual Property Theft, Data Leakage


**Data Analytics using IoT**

**Making Things Smart:** Getting Things onto the Internet

IoT in Home, Cities/Transportation, Retail, Healthcare, Sports

**References:**

1. “Learning Internet of Things” by Peter Waher, Packt publisher
2. “Practical Internet of Things Security” by Brian Russell, Drew Van Duren, Packt publisher
3. “Raspberry Pi with Java: Programming the Internet of Things (IoT)” by James L. Weaver and Stephen Chin, Oracle Press
4. “The Internet of Things (The MIT Press Essential Knowledge series)”, By Samuel Greengard
5. “The Silent Intelligence: The Internet of Things”, by Daniel Kellmereit and Daniel Obodovski
ISI9: SCADA Security


Text books:


*****
**Stream: Information Security Management - Suggestive Course Codes (ISEA-MT- ISMX)**

**ISM1: Information Security Risk Management**

Development of concepts required for risk-based planning and risk management of computer and information systems (Risk analysis, risk perception, Communicating risk, risk mitigation); Objectives and methods for vulnerability assessment for natural disaster, technological hazards, and terrorist threats; implications for emergency response, vulnerability of critical infrastructures;

References:

**ISM2: Public Key Infrastructure and Trust Management**

Public Key Infrastructure - components and architecture. PKI interoperability, Deployment and Assessment of PKI data structures; Certificates; Validation; Revocation; Authentication; Cross-certification. Repository, Certification Authority (CA) and Registration Authority (RA), trusted third party, digital certificates.

PKI Services – Authentication, non-repudiation, privilege management, privacy, secure communication.

Key management – certificate revocation list, root CA, attacks on CA, key backup. PKI standards – SSL, LDAP, IPSec, X.500, X.509, S/MIME

Trust models – strict v/s loose hierarchy, four corners, distributed. Certificate path processing – path construction and path validation.

References:
1. Understanding PKI: Concepts, Standards, and Deployment Considerations; Carlisle Adams, Steve Lloyd; Addison-Wesley Professional, 2003
2. Access Control, Authentication, and Public Key Infrastructure; Bill Ballad, Tricia Ballad, Erin Banks; Jones & Bartlett Publishers, 22-Oct-2010

**ISM3: Cyber laws and rights in the digital age**

IT Act; The rights the various parties have with respect to creating, modifying, using distributing, storing and copying digital data - concurrent responsibilities and potential liabilities; Intellectual Property Issues connected with use and management of Digital Data. The similar Acts of other countries will also be discussed.

References:
1. Managing Cyber Attacks in International Law, Business, and Relations: In Search of Cyber Peace; Scott J. Shackelford; Cambridge University Press, 10-Jul-2014
2. Cyberlaw: the Indian perspective; Pavan Duggal; Saakshar Law Publications, 2002

**ISM4: Computer Security Audit and Assurance**

Security Policy frameworks: practices, and procedures, business practice disclosures, Policy authority and practices, information security practices, personal and physical security practices, operation management practices, PKIs and key management schemes, key generation, key storage, backup, recovery and distribution, XML frameworks for security policy specification, certificate management life cycle.

References:
1. Information System Audit and Assurance; D. P. Dube, Ved Prakash Gulati; Tata McGraw-Hill Education, 01-Jan-2005
2. Auditing IT Infrastructures for Compliance; Martin Weiss, Michael G. Solomon; Jones & Bartlett Publishers, 10-Jul-2015

**ISM5: Strategic Computing and Communication Technology**

(Competitive strategies for the information economy, network economics) Telecommunications and networking as applied to enterprises in the commercial and public sector, A survey of the technologies and applications of telecommunications systems with emphasis on LANs and Internet technologies, selection of technologies and configurations necessary to support business applications

Competitive, economic, and political factors that influence technology innovation in public and private organizations, domestically and internationally, Management of research and development: project selection, resource allocation, technology planning, management of development projects. Quality, manufacturing, and intellectual property issues

**References:**

“To be adopted by the course instructor”

**ISM6: Security Engineering for Business Computing**

Introduction to Security Engineering; Passwords and their limitations, attacks on Passwords; CAPTCHA

**Access Control:** ACL, sandboxing, virtualization, trusted computing; Multi-level and Multi-lateral security

**Digital Certificates and PKIs, Different PKIs:** PGP (Pretty Good Privacy)- Web of trust, applications X.509: X.500, Certification Authority (CA), Registration Authority (RA), Root - CA, X.509 Protocols, Hierarchy of Trust, Simple PKI (SPKI) / Simple Distributed Security Infrastructure (SDSI); Access Control Mechanisms including Role based access control. Issues of revocation, Anonymity and Privacy issues Smartcard integration with PKIs Trust Management Systems, Risks Impact on E-Commerce and E- Business

**Biometrics:** Security via biometrics, Spaced Domain based biometric and recognition techniques; Correlation based biometric filters, Basic theory of Correlation filters; Design of advanced correlation filters that offer tolerance to expected impairments; Methods to implement digital correlations; Applications of correlation filters

**Securing services:** Security in Metered Services, pre-payment meters. Secure printing and Seals. Tamper resistance mechanisms. Auctions and Trading Mechanisms, safe exchange, payment mechanisms and protocols, Searching hyperlinked structures, data mining, copyright protection and security, web software infrastructure, personalization and tracking, integration of catalogs and other trading information

**References:**

“To be adopted by the course instructor”

*****
ISP1: Formal Methods for Protocol Analysis

Protocol analysis tools: Finite-state checking (Murphi), Infinite-state symbolic analysis (SRI constraint solver), Probabilistic model checking (PRISM), Game-based verification (MOCHA), Process algebras (Spi-calculus and applied pi-calculus), Protocol logics (BAN, DDMP, Isabelle), Probabilistic polynomial-time calculus, CSP, B-method approach, Strand spaces, Inductive approach.

Communicating Sequential Programming: Basic building blocks, Parallel operators, Process behavior, Modeling security protocols in CSP - Trustworthy processes, Modelling an intruder, protocol goals

Transformations: Transformations on protocols, Safe simplifying transformations, Structural transformations

Formal analysis: Formal definitions of security for symmetric ciphers, Formal model for secure key exchange

Theorem proving - Rank functions, Secrecy of shared key, Authentication

Secure systems: hardware, software and communication systems – design issues and analysis

Secure software Architecture: models and principles, hardware design related security – smart cards and other security solutions, communication protocols and application systems associated with security

References:

“To be adopted by the course instructor”

ISP2: Operating System Design and Architecture

Introduction to operating systems, Abstract view of an operating system

OS evolution: multi-programming, time-sharing, Dual-mode operation, Protecting I/O, memory, CPU, kernels and micro-kernels, elementary computer architecture.

Processes and scheduling Job/process concepts

Scheduling basics: CPU-I/O interleaving, (non-)preemption, context switching

Scheduling algorithms: FCFS, SJF, SRTF, priority scheduling, round robin, Combined schemes

Memory management: Processes in memory, Logical addresses

Partitions: static versus dynamic, free space management, external fragmentation, Segmented memory

Paged memory: concepts, internal fragmentation, page tables. Demand paging/segmentation

Replacement strategies: OPT, FIFO, LRU (and approximations), NRU, LFU/MFU, MRU; Working set schemes; I/O subsystem, General structure, Polled mode versus interrupt-driven I/O

Application I/O interface: block and character devices, buffering, blocking versus non-blocking I/O. Other issues: caching, scheduling, spooling, performance; File management; File concept; Directory and storage services; File names and meta-data

Directory name-space: hierarchies, DAGs, hard and soft links; File operations; Access control; Existence and concurrency control Protection; Requirements, Subjects and objects; Design principles, Authentication schemes,

Access matrix: ACLs and capabilities; Combined scheme; Covert channels


Processes: memory image, life cycle, start of day. The shell: basic operation, commands, standard I/O, redirection, pipes, signals. Character and block I/O. Process scheduling

References:


**ISP3: Advanced Operating System Design**


Distributed OS - Issues & Challenges

**References:**

“To be adopted by the course instructor”

**ISP4: Simulation and Modelling**

Definition of a system; System concepts, type of system; Continuous & Discrete systems; Modeling process verification & validation
Markov chains- Weak law of large numbers; Central limit theorem; Strong law of large numbers; Queuing models;
Little’s Theorem, M/M/1, M/M/m, M/M/, M/M/m/m, M/G/1,and M/M/1/J queuing systems.
Introduction to Simulation Models; Classification of simulation models; Advantages and Disadvantages of simulation;
Discrete system simulation: Monte Carlo method, Random number generators, Probability Distributions.
Element of inventory theory, more complex inventory models, finite & infinite delivery rate model with and without back ordering; Simulation of Inventory Systems

**References:**

“To be adopted by the course instructor”

**ISP5: Optimization Techniques**

**Introduction:** Introduction, Engineering applications (models) of optimization.

**Linear Programming:** Graphical, simplex method, Concept of duality, Dual simplex method. Dynamic Programming:

**Transportation Problems:** basic feasibility solution by different methods, optimal solution, Degeneracy in transportation problem, unbalanced transportation problems.

**Assignment Problems:** Balanced and unbalanced Assignments; Assignments to given schedule. Introduction to Non-linear programming

**References:**

“To be adopted by the course instructor”

**ISP6: Web Architecture Security**

Web security model - Browser security model including same-origin policy, Client-server trust boundaries, e.g., cannot rely on secure execution in the client

Session management, authentication-Single sign-on, HTTPS and certificates

Application vulnerabilities and defenses- SQL injection, XSS, CSRF

Client-side security - Cookies security policy, HTTP security extensions, e.g. HSTS, Plugins, extensions, and web apps, Web user tracking

Server-side security tools, e.g. Web Application Firewalls (WAFs) and fuzzers

**Major Browser Attacks**
References:

ISP7: Advanced Distributed System

Synchronization: Clock synchronization - mutual exclusion - electronics atomic transactions - dead locks. Process and Processors: Threads - System models processor allocation - scheduling fault tolerance - real time distributed systems.
Distributed file systems: File system design and implementation - trends in distributed file systems.
Shared Memory: Introduction - bus based multi processors ring based multiprocessors switched multiprocessors - NUMA comparison of shared memory systems - consistency models - page based distributed shared memory - shared variable distributed shared memory - object based distributed shared memory. Case studies: MACH and CHORUS

References:

“To be adopted by the course instructor”

*****
Stream: Analysis - Suggestive Course Codes (ISEA-MT- ISAX)

ISA1: Protocol Analysis


Protocol analysis tools: Finite-state checking (Murphi), Infinite-state symbolic analysis (SRI constraint solver), Probabilistic model checking (PRISM), Game-based verification (MOCHA), Process algebras (Spi-calculus and applied pi-calculus), Protocol logics (BAN, DDMP, Isabelle), Probabilistic polynomial-time calculus, CSP, B-method approach, Strand spaces, Inductive approach.

Communicating Sequential Programming: Basic building blocks, Parallel operators, Process behavior, Modeling security protocols in CSP - Trustworthy processes, Modelling an intruder, protocol goals.

References:

“To be adopted by the course instructor”

ISA2: Digital Watermarking and Steganalysis


Steganography – Least Bit, DCT, Spread spectrum. Audio steganography, Steganalysis techniques

References:

“To be adopted by the course instructor”

ISA3: Data Mining and Machine Learning

Data Mining: Introduction and need, Descriptive and Predictive Data Mining.

Data Processing: Data Cleaning, Data Integration and Transformation, Data Reduction.

Data Mining Primitives: Language DMQL and its Preliminary Clauses.

Data Mining Methods: Association – Single and Multilevel, Characterization and Comparison, Regression Analysis, Classification and Predication.

Data Mining Algorithms: Clustering, Association, Regression, Decision Trees

Overview of Machine Learning: Concept Learning, Version spaces, Inductive Bias, Induction of Decision Trees, overfitting, pruning, Evaluating Hypotheses, Bayesian Learning, Bayes Optimal Classifier, Naïve Bayes Classifier; Bayesian Networks. Computational Learning Theory, Instance-Based Learning, k-Nearest Neighbour Learning, Locally Weighted Linear Regression, Genetic Algorithms, Genetic Programming. Learning Sets of Rules, Analytical Learning, Reinforcement Learning, PAC models, hidden Markov models, Genetic algorithms

Textbooks/ references:


**ISA4: Privacy and Security for Online Social Networks**
Introduction to Online Social Networks, data collection from social networks, challenges, opportunities, and pitfalls in online social networks, APIs; Collecting data from Online Social Media, Trust, credibility, and reputations in social systems; Trust, credibility, and reputations in social systems; Online social Media and Policing, Information privacy disclosure, revelation and its effects in OSM and online social networks; Phishing in OSM & Identifying fraudulent entities in online social networks

References:

“To be adopted by the course instructor”

**ISA5: Decision Support Systems and Methods**
Computer-based decision-making aids and simulations; Issues in effective implementation of decision support systems, Review and analysis of various expert systems, including tools and generators, classification vs diagnostic type systems, and building module, Design of decision support and expert systems, Use of the Management Decision Center to investigate group dynamics in decision making. Methods of dealing with unstructured and under-specified problems from management and organizational perspectives, the role of the facilitator in group decision-making

References:

“To be adopted by the course instructor”

**ISA6: Malware Analysis**

Text books / references:

******
Stream: Cybercrime Investigation and Forensics - Suggestive Course Codes (ISEA-MT- ISFX)

**ISF1: Cyber Crime and Information Warfare**

Cyber Crime: Industrial espionage and cyber-terrorism, principles of criminal law, computer forensic investigation, elements of personnel security and investigations, principles of risk and security management, conspiracy in computer crime, and computer fraud investigation.


Information Warfare: Nature of information warfare including computer crime and information terrorism; Threats to information resources, including military and economic espionage, communications eavesdropping, computer break-ins, denial-of-service, destruction and modification of data, distortion and fabrication of information, forgery, control and disruption of information flow, electronic bombs, and perception management.

Defenses: Countermeasures including authentication, encryption, auditing, monitoring, intrusion detection, and firewalls, and the limitations of those countermeasures. Introduction to Open Source Intelligence (OSINIT), web intelligence and social media intelligence

Cyberspace law and law enforcement, information warfare and the military, and intelligence in the information age

**References:**

1. Information Warfare, Ventre, John Wiley & Sons, 15-Feb-2016

**ISF2: Computer Crime Investigations and Cyber Forensics**

Framework for Digital Forensic Evidence Collection and Processing, Fundamentals of Host Forensics for Microsoft Windows - Kernel and Device driver architecture, registry, auditing and security architecture

File system handling - Reconstruction of files and directory structures on the FAT and NTFS

Fundamentals of Host Forensics for UNIX derivatives - Linux operating system, Kernel and Device drives architecture, Security and audit mechanisms, file system and pseudo file systems, the reconstruction of file and directory structures using UFS and Ext2/3fs as exemplars.


**Text books/references:**


**ISF3: Cyber laws and rights in the digital age**

IT Act; The rights the various parties have with respect to creating, modifying, using distributing, storing and copying digital data - concurrent responsibilities and potential liabilities; Intellectual Property Issues connected with use and management of Digital Data. The similar Acts of other countries will also be discussed
References: “To be adopted by the course instructor”

ISF4: Advanced Forensics

Basic Principles and methodologies for digital forensics, Design systems with forensic needs in mind, Rules of Evidence – general concepts and differences between jurisdictions and Chain of Custody, Search and Seizure of evidence: legal and procedural requirements, Digital Evidence methods and standards
Techniques and standards for Preservation of Data, OS/File System Forensics
Application Forensics, Web Forensics, Network Forensics, Mobile Device Forensics, Computer/network/system attacks, Attack detection and investigation
Anti-forensics

References: “To be adopted by the course instructor”

ISF5: Incident Response and Cyber Forensics


Textbooks/ references:


*****
Career Options in different streams of specializations

I. Cryptography

A. About Cryptologist
Cryptologists before the 80s were primarily depicted as spy agents involved in deciphering and configuring coded messages to gain momentum against enemy activities. However, with the upsurge of information technology and the increasing dependence on electronic data processing, the range of activities a cryptologist is involved in has expanded. The vast digital data that is stored and processed in large computer bases and transmitted through complex communication networks is susceptible to unauthorized interception and interpretation and hence, needs to be protected through encrypted remote access or passwords. "Our commercial transactions (credit card numbers and bank data), our medical data (which may soon be stored on smart cards), mobile communication and other secret diplomatic information can be traced by hackers. To prevent such data theft, we need cryptographers to write stronger codes. In fact, currently, cryptography has broadened greatly from the study of secret writing to the study of information security.

A Cryptologist is someone who is skilled at deciphering codes, puzzles or cryptograms, and at creating them in order to protect private information. Cryptologists not only decipher codes or cryptograms, but they also invent them. Cryptologists create secret codes used for communicating military secrets, protecting government, medical and other private information, disguising spy communications, and for encrypting our own personal information to protect it from prying eyes on the Internet.

B. Who do they work for
- Many Cryptologists work for Technology companies such as Google, Microsoft; Payment Gateways such as Paypal; Credit card companies; online payment companies or any company responsible for managing private personal customer information.
- Cryptologists are in demand in the military forces, government agencies, law enforcement agencies, universities and research institutes. Depending on the profile of the organization one is involved with, the area of functioning varies. In these organizations, their roles vary from being theoreticians (people who study cryptograms and algorithms and develop theories about them) to being a part of military intelligence (creating algorithms to disguise military communications, and trying to break the codes of other countries military intelligence) to gang taskforce officers (cops who break gang code to discover locations and dates of criminal activity).

C. Suitable Job Titles in the area of Cryptography area could be
Cryptanalyst, Cryptographer, Cryptologic Technician, Cryptologic Linguist, Symbolist, Decipherer, Information Security Expert, Intelligence Agent or Officer, Information Security Engineer

D. How M Tech (IS) prepare student for career in the area of Cryptography
- Core Modules are designed keeping depth of cryptography in view
- Diverse subjects are being offered to cater to many career options in the area of Cryptography
- Inbuilt internship program and project work
II. Data Privacy

A. About Data Privacy Engineer
A Data Privacy Engineer will be trained to design cutting edge products and services that leverage big data while preserving privacy. They have to identify points where privacy may be at risk, and propose and evaluate solutions to mitigate these risks. They need to understand the capabilities and limitations of privacy enhancing technologies. They use techniques to aggregate and de-identify data, understand the limits of de-identification and how data might be re-identified, and understand concepts such as k-anonymity and differential privacy. They have to understand the current privacy regulatory and self-regulatory frameworks. They are in line with current technology-related privacy issues including tracking for online behavioral advertising, location tracking, frictionless sharing, and emerging issues. They have to conduct privacy-related risk assessments and compliance reviews, respond to incidents, and integrate privacy into the software engineering lifecycle phases. They also required conducting basic usability evaluations to assess the usability and user acceptance of privacy-related features and processes.

Privacy Engineer / Managers are serving as an effective privacy subject matter expert to help interdisciplinary teams simultaneously address legal, engineering, user interface, business, marketing and other requirements

B. Who do they work for
- Data Privacy Engineers / Managers are work in the servicing industries such as IBM, HP, Infosys, Payment Card Industry, Banking where legal and the audit framework as mandate for their customer information.
- They majorly work in the Law enforcement where creating legal framework for the Cyber relating fields

C. Suitable Job Titles in the area of Privacy area could be
Data Privacy Engineer, Privacy Manager, Information Security Manager, Privacy Expert, Law and Privacy Manager

D. How M Tech (IS) prepare student for career in the area of Data Privacy
- Core Modules are designed keeping depth of information security in view
- Different topics in the Cyber Law and Cybercrime subjects are being offered to cater to career options in the area of Data Privacy
- Inbuilt internship program and project work
III. Security Operations & Management

A. About Security Operations & Management
Students who trained in the area of Security will be prepared to be a Security Operations Manager and has the responsibility include risk management assessments, as well as ensuring Compliance with local, state, and Government guidelines regarding emergency and security. The operation manager also will serve as liaison with local law enforcement to assist investigations of accidents, thefts, and property loss. Operation Manager will hire, train, and coordinate work schedules of all security personnel to ensure a secure environment at all locations and all times. Operation Manager will establish security objectives, goals, processes, and plans in support of divisional and corporate strategic directions. Operation Manager is responsible for advising and counseling management on their compliance posture to all division and corporate standards. Sound judgment is required as decisions made are often major and affect relationships with customers, vendors, suppliers, and employees.

Operation Manager must have a comprehensive knowledge and understanding of asset and information protection principles necessary to plan and implement security programs and solutions in support of the business. Operation Manager have strong management presentation and negotiation skills as well as proven experience in organizing and directing staff/team work and coordinating such activities to a successful conclusion. Requires strong analytical and problem solving skills to review, evaluate, recommend changes and/or develop and implement new programs as requirements and customer needs change. Must have the skill and ability to conduct and/or support sensitive investigations involving company personnel, assets, and/or proprietary information.

B. Who do they work for
- Infrastructure service oriented companies such as Microsoft, HP, IBM, Verizon, Infosys, WIPRO, CISCO, Juniper etc.
- Internet Service Providers such as Alcatel, Verizon, Airtel, Vodafone etc.

C. Suitable Job Titles in the area of Security and Operations area could be
Security Engineer, Operations Manager, Information Security Specialist, Information Security Analyst

D. How M Tech (IS) prepare student for career in the area of Security and Operations
- Core Modules are designed keeping depth of information security in view
- Different topics in the infrastructure and Communication subjects are being offered to cater to career options in the area of Data Privacy
- Inbuilt internship program and project work
IV. Cyber Forensics

A. About Security Operations & Management
Students who are aware of Forensic Sciences, Legal Systems, Crime Prevention Techniques, Investigative Methods must take the knowledge and able to do the following:
- Every individual must have knowledge about Forensic Practices to protect evidences and to help crime investigation process
- Be your own Crime Investigator in different fields of Forensic Sciences
- Being Crime Investigator or Forensic Scientist, you will help to nation for crime investigation, crime prevention and to decrease crime rate
- This Course will help you start your own Forensic Practice, Career & Forensic Services, Investigation, Detective agency or consultancy
- Indicates skill and expertise levels and Progressing more quickly on your career journey
- This Courses guides through a complete method for Forensic Investigation, Legal Framework and procedures

B. Who do they work for
- Forensic Engineers / Managers are work in the servicing industries such as IBM, HP, Infosys, Payment Card Industry, Banking where legal and the audit framework as mandate for their customer information.
- They majorly work in the Law enforcement where creating legal framework for the Cyber relating fields

C. Suitable Job Titles in the area of Forensics area could be
Forensics Engineer, VA/PT Test Engineer, etc.

D. How M Tech (IS) prepare student for career in the area of Forensics
- Core Modules are designed keeping depth of information security in view
- Different topics in the Cyber Law, Cyber Forensics studies and Cybercrime subjects are being offered to cater to career options in the area of Data Privacy
- Inbuilt internship program and project work

*****
## Information Security Education and Awareness Project – Phase II

### 6 month / 1 year PG Diploma Courses

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>ISEA 101 Fundamental of Computers</td>
<td>ISEA 201 Security Concepts</td>
<td>ISEA 301 Network Defense and Countermeasures (NDC)</td>
</tr>
<tr>
<td>ISEA 102 Fundamentals of Computer Networks</td>
<td>ISEA 202 Network Security</td>
<td>ISEA 302 Firewalls and IDS</td>
</tr>
<tr>
<td>ISEA 103 Concepts of Operating System and Administration</td>
<td>ISEA 203 Java Programming with Crypto API</td>
<td>ISEA 303 Cyber Forensics &amp; Cyber Laws</td>
</tr>
<tr>
<td>ISEA 104 Windows Administration and Management</td>
<td>ISEA 204 Database Security</td>
<td>ISEA 304 Switching and Router Security</td>
</tr>
<tr>
<td>ISEA 105 Linux Administration and Management</td>
<td>ISEA 205 Web Application Security</td>
<td>ISEA 305 Ethical Hacking</td>
</tr>
<tr>
<td>ISEA 106 IT Infrastructure Management</td>
<td>ISEA 206 Mobile Application Security</td>
<td>ISEA 306 Advanced security Management in Cloud computing with Virtualization</td>
</tr>
<tr>
<td>ISEA 107 Computer Organization &amp; Architecture</td>
<td>ISEA 207 Public Key Infrastructure and Cryptography</td>
<td>ISEA 307 Data Center management &amp; Security Administration and Security Operations</td>
</tr>
<tr>
<td>ISEA 109 Scripting Languages for Information Security</td>
<td>ISEA 209 Web/Network/Wireless Penetration testing</td>
<td>ISEA 309 Security over Internet of Things</td>
</tr>
<tr>
<td>A. HTML</td>
<td>ISEA 210 Introduction to Malware Reverse Engineering technologies and Methodologies</td>
<td>ISEA 3010 Security Analytics for Big Data</td>
</tr>
<tr>
<td>B. PHP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C. Java Script</td>
<td></td>
<td></td>
</tr>
<tr>
<td>D. Python</td>
<td></td>
<td></td>
</tr>
<tr>
<td>E. Perl</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISEA 1010 Secure Programming methodologies</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Course Curriculum

Basic Systems/ Security Management Courses – Core Courses

ISEA 101 Fundamental of Computers

Course Contents

- Introduction to Computer Fundamentals and Computer Networks Overview of PC architecture.
  - Switch Mode Power Supply: Discrete components, principle of operation SMPS, converter topologies, PWM IC’s and case study.
  - Monitors: Monitors:- CRT, LCD and LED Displays CRT construction and working, 9 pin input type monitor, block diagram of colour monitor.
  - Keyboard: Block diagram of keyboard circuit.
  - Printer: Types & components of printers, printer interface with computer, detailed circuit study of Dot Matrix Printer, function block diagram for various sub-assemblies of printer, principle of operation of Laser and Inkjet printers, various mechanical sub-assemblies, general maintenance aspects.
- Different bus standards (ISA, PCI, PCMCIA), Different Add-on Cards like memory, Graphics and other add-on cards.
- NIC, USB devices, Optical storage, solid-state devices
- Troubleshooting issues related to Memory, Display and CPU problems System Maintenance

ISEA 102 Fundamentals of Computer Networks

Course Contents

  - Physical Layer: transmission media, analog transmission, digital transmission.
  - Data Link Layer: Framing, Error detection and correction, Stop-and-wait protocol, sliding window protocols.
    - MAC Layer: Aloha protocols, CSMA/CD; Ethernet, Token ring, Token bus.
    - Logical link control. May be some other MAC protocols like, FDDI, Gigabit Ethernet, wireless, etc.
  - Routing protocols (examples: RIP, HELLO, OSPF, BGP). Classless
  - Inter-Domain Routing – Congestion Control Algorithms. Multicasting. Other protocols: ICMP. ARP, RARP, BOOTP, DHCP.
  - Transport Layer – Flow and error control, multiplexing, establishing and releasing a connection.
- Introduction to UNIX network programming & socket abstraction. Client-server architecture.
- Session, Presentation, Application Layers.
ISEA 103 Concepts of Operating System and Administration

Course Content
- Introduction.
- Process management: process synchronization and mutual exclusion, two process solution and Dekker's algorithm, semaphores, examples (producer-consumer, readers-writer, dining philosophers, etc.).
- CPU scheduling: multiprogramming and time sharing, scheduling approaches (SJF, FIFO, round robin, etc.).
- Input/Output: device controllers and device drivers, disks, other devices.
- Memory management: with and without swapping, virtual memory - paging and segmentation, page replacement algorithms, implementation.
- File systems: FS services, disk space management, directory and data structure.
- Deadlocks: modeling, detection and recovery, prevention and avoidance.
- Example Systems: LINUX/BSD, Windows

ISEA 104 Windows Administration and Management

Course Content
- Installation and configuring the Windows servers
- Active directory configuration, Trusts and relationships, organizational units, group policies
  - Installing Active Directory, Configure and manage Active Directory, Configure service authentication, Create and configure Service Accounts; create and configure Group Managed Service Accounts; create and configure Managed Service Accounts; configure Kerberos delegation; manage Service Principal Names (SPNs), Installing Active Directory. What is DNS? What does DNS have to do with Active Directory? DNS domain names and naming conventions. Installing DNS for Active Directory, creating and configuring DNS zones, configuring zone transfers Removing Active Directory. Verifying and troubleshooting an Active Directory installation.
  - Configure Domain Controllers, Configure Universal Group Membership Caching (UGMC); transfer and seize operations masters; install and configure a read-only domain controller (RODC); configure Domain Controller cloning
  - Maintain Active Directory, Back up Active Directory and SYSVOL; manage Active Directory offline; optimize an Active Directory database; clean up metadata; configure Active Directory snapshots; perform object- and container-level recovery; perform Active Directory restore.
- Software Deploy and manage server images:
  - Windows Deployment Services (WDS) role; configure and manage boot, install, and discover images; update images with patches, hotfixes, and drivers; install features for offline images, Implement patch management: Install and configure the Windows Server Update Services (WSUS) role; configure group
policies for updates; configure client-side targeting; configure WSUS synchronization; configure WSUS groups are deployments, Managing disks

- **Windows Security Management**
  - LSA Policy, Password Filters, Safer, Service Security Attachments

- **Backup & Recovery:**
  - User data and system state, data backup types. Backup strategies, scheduling, recovering user data and system state, data recovering from a system failure. Using the recovery console to restore a system, using the emergency repair disk to restore a system.

**ISEA 105 Linux Administrations and Management**

*Course Content*

- Installation and configuring the Linux.
- Introduction to Basic commands, File system hierarchies, startup & shutdown files, Package administration
- RAID and LVMS, NFS, NIS, FTP & SAMBA, Ext2/3/4, GFS, PFS
- DNS, DHCP, Send mail, Apache configuration and Management, Nginx
- Disk quotas, job scheduling, and squid
- TCP WRAPPERS, PAM modules
- Systems Concepts
- Bash Scripting
- Linux Security Services Management
- Shell Scripting
  - sed, awk, bash scripting
  - Perl language
  - Perl for Linux Administration
  - Perl for Windows Administration

**ISEA 106 IT Infrastructure Management**

*Course Content*

- Introduction to ITIL
  - Service Strategy, Service Design, Service Transition, Service Operation, Continual Service Improvement
- Data Center Management
  - Introduction to DCM, Data Center design, Server Security, Storage area network, Physical security, LXC, Docker, Vagrant, KVM, Hyper-V, Bare-metal, Introduction Virtual Private Cloud (VPC) Setup,
Bootstrapping Chef/puppet Server, Writing basic Chef recipes, Centralized logging (nagios), Munin, Statsd, Graphite, Load testing (proving you can handle more traffic), Identifying bottlenecks, Auto-scaling Auto-rebuilding old instances, Updating without downtime, Auto-healing

ISEA 107 Computer Organization & Architecture

Course Content
- Memory: organization inside a memory chip, interfacing of memory with processor; Bus protocols;
- Number representation: integer representation, character representation, real number representation
- Processor organization: computer arithmetic, adders - ripple carry and carry look-ahead, multipliers, ALU design, control structure, hardware, microprogramming, nano programming, assembly language programming
- Input Output organization: program controlled, interrupt driven, DMA driven
- Computer peripheral organization: keyboard design and processor interface, hard disk design and processor interface, floppy disk drive and processor interface, VDU and concept of graphics adapters. Printers: dot matrix, line printer and laser printer
- Pipelining – Introduction of virtual memory and cache systems; Newer features, e.g., RISC, parallel architectures, etc.

ISEA 108 Mobile & Wireless Security Management

Course Content
- Mobile Computing (MC): Introduction to MC, novel applications, limitations, and architecture
- GSM: Mobile services, System architecture, Radio interface, Protocols, Localization and calling, Handover, Security, and New data services
- (Wireless) Medium Access Control: Motivation for a specialized MAC (Hidden and exposed terminals, Near and far terminals), SDMA, FDMA, TDMA, CDMA
- Mobile Network Layer: Mobile IP (Goals, assumptions, entities and terminology, IP packet delivery, agent advertisement and discovery, registration, tunneling and encapsulation, optimizations), Dynamic Host Configuration Protocol (DHCP)
- Mobile Transport Layer: Traditional TCP, Indirect TCP, Snooping TCP, Mobile TCP, Fast retransmit/fast recovery, Transmission /time-out freezing, Selective retransmission, Transaction oriented TCP. Database Issues: Hoarding techniques, caching invalidation mechanisms, client server computing with adaptation, power-aware and context-aware computing, transactional models, query processing, recovery, and quality of service issues
- Data Dissemination: Communications asymmetry, classification of new data delivery mechanisms, pushes based mechanisms, pull-based mechanisms, hybrid mechanisms, selective tuning (indexing) techniques. Mobile Ad hoc Networks (MANETs): Overview, Properties of a MANET, spectrum of MANET applications, routing and various routing algorithms, security in MANETs
- Protocols and Tools: Wireless Application Protocol-WAP. (Introduction, protocol architecture, and treatment of protocols of all layers), Bluetooth (User scenarios, physical layer, MAC layer, networking, security, link management) and J2ME
- Wired/wireless networks; Effect of mobility on networks, & systems; impact on IP stack from MAC layer and up; ad-hoc and sensor networks; wireless broadcast, IP broadcast, Satellite broadcast; issues of information capacity; distinction between wired and wireless networks from information theory; Issues of security in wireless; issues of 802.11 protocols; routing in wireless networks, design of secure protocols: key distribution for access control, source authentication of transmissions, and non-repudiation; Power
management and selfishness issues, attacks in wireless networks; DOS and DDOS attacks, reaction to attacks, information processing for sensor networks

ISEA 109 Scripting Languages for Information Security

Course Content

HTML
- Introduction to HTML
- What is HTML, HTML Documents, Basic structure of an HTML document, Creating an HTML document, Mark up Tags, Heading-Paragraphs, Line Breaks,

PHP
- PHP installation and Introduction
- Loops String Functions in PHP
- PHP Email Function PHP Basics,
- Variables Arrays in PHP with Attributes Date & Time,
- Image Uploading File handling in PHP Functions in PHP
- Errors handling in PHP

JavaScript

Python

Perl
- Introduction to Perl – Overview of Perl Features, Getting and Installing Perl, Accessing Documentation via perldoc, HTML-Format Reference Documentation, Perl Strengths and Limitations
- Security Issues in Perl Scripts

NodeJS
- Introduction to Node.js; Events; Streams; Modules; Express; Socket.io; Persisting Data

ISEA 1010 Secure Programming methodologies

Course Content

- Security Programming and Techniques - Intelligent source code reuse, Legacy problems, Security input and output handling, Canonicalization, Low tolerance against "potential" bug

******
**ISEA 201 Security Concepts**

*Course Content*

- Introduction: need and basic goals for computer security, security threats etc.
- Operating System Security: low-level protection mechanisms, access control: models for access control, some confidentiality, integrity, and hybrid models of access control such as Bell-La Padula, Biba, Chinese Wall etc., discretionary v/s mandatory access control
- Case studies: Java access control policy specifications, SELinux - security model and implementation
- Program flaws: bugs which have security implications such as buffer overflows, race conditions and etc.
- Malicious code: viruses, worms, Trojan horses; how they work and how to defend against them
- Authentication and authorization techniques. Passwords, shadow files, one-time passwords, Bio-metric based identification and authentication systems. Smart cards. Kerberos
- Other topics:
  - Dealing with spam. Secure email systems. PGP, SMIME, DKIM, DMARC, DNSSec, SMTP STS etc.
  - Covert channels
  - Disaster management

**ISEA 202 Network Security**

*Course Content*

- Key exchange protocols. Diffie-hellman and its variants. Man in the middle attack. PKI and certificate based key exchange and Key management
- Protocol weaknesses in IP/TCP and other protocols. Various types of attacks
- Security protocols at application level: PGP, HTTPS, SSH, DNSSec, eSMTPS etc.
- Security protocols at socket layer: SSL/TLS
- Security protocols at network layer: IPSec
- Security protocols for remote connections through dial-up etc.: PPTP, L2TP
- Firewalls and packet filtering
- Proxy or application level gateways as security devices
- Virtual private networks
- Intrusion Detection Systems
- Privacy protection and anonymity services
- Electronic payment system

**ISEA 203 Java Programming with Crypto API**

*Course Content*

- **Introduction to Java**
  - Java Overview, Data types, Arrays, Decision statements, Loops, Classes, Package, java.lang, java.util, Java Interfaces, Exception Handling, Networking with Java, JSP & Servlets
- **Cryptography**
  - Java Cryptography Architecture, Java Cryptography Extension, SSL and TLS protocols, A Basic of SSL client and Server, Client side Authentication, Managing SSL Session Information, Dealing with HTTPS
- **Secure Coding with Java**
  - Fundamentals, Denial of Service, Injection and Inclusion, Buffer Overflows and Input Validation, Access Control

**ISEA 204 Database Security**

*Course Content*
- Database design and use of DBMS, Relational models and Relational algebra and design principles, network models, object-oriented design, transaction processing, Datalog, temporal databases, advanced topics from data warehousing, knowledge discovery, data mining, middleware etc.

**ISEA 205 Web Application Security**

*Course Content*
- Application Security – HTTPS, HSTS, SMIME, PGP, SET, E-mail and IM security, DNSSec, eSMTPS, DKIM, DMARC, DNSSec, SMTP STS
- Secure Configuration of Applications: Web Server, Database Server, Email Server, etc.
- Security protocols at application level: PGP, HTTPS, SSH, etc.
- Proxy or application level gateways as security devices
- Top 10 OWASP Vulnerabilities and Countermeasures

**ISEA 206 Mobile Application Security**

*Course Content*
- Introduction to Mobile Security Management
  - Identifying components of a mobile Operating System (OS)
  - Recognizing application security challenges
  - Exposing the threats faced by mobile devices
  - Discovering mobile hacking tools
- Evaluating vulnerabilities
  - Exploring multiple and diverse device environments
  - Recognizing the risks of mobile applications
  - Defining methods for determining vulnerabilities
  - Uncovering common device configuration errors
- Integrating Security throughout the Application Development Process
  - Applying secure development guidelines
  - Leveraging Xcode and Eclipse ADT
  - Implementing secure coding techniques
  - Differentiating between software and programming language vulnerabilities
- Employing Open Web Application Security Project (OWASP) resources
  - Revealing the top mobile risks
  - Addressing identified exploits promptly
  - Defeating client-side injection attacks
  - Debugging a running app in an emulator
  - Reverse-engineering apps to identify vulnerabilities
- Implementing mobile application security
  - Protecting user interface data
 ✓ Storing data in the Android and iOS Keychain
 ✓ Enforcing user authentication
 ✓ Handling sessions properly
 ✓ Defining trust boundaries

ISEA 207 Public Key Infrastructure and Cryptography

Course Content

- Digital Certificates and PKIs
- Different PKIs:
  ✓ PGP (Pretty Good Privacy)- Web of trust, applications
  ✓ X.509: X.500, Certification Authority (CA), Registration Authority (RA), Root - CA
  ✓ X.509 Protocols, Hierarchy of Trust, Simple PKI (SPKI) / Simple Distributed Security
  ✓ Infrastructure (SDSI); Access Control Mechanisms including Role based access control
- Issues of revocation, Anonymity and Privacy issues
- Smartcard integration with PKIs
- Theory, foundations, and applications of modern cryptography, Steganography, One-way functions; pseudo-randomness and random number generators; encryption; authentication; symmetric cryptography, asymmetric cryptography: public-key cryptosystems; digital signatures, message authentication codes, remote user authentication, notions of security; - zero-knowledge/interactive proofs, multi-party cryptographic protocols, key exchange and applications; cryptanalysis of cryptographic primitives and protocols, such as by side-channel attacks, differential cryptanalysis, or replay attacks; and cryptanalytic techniques on deployed systems etc.

Biometric Security

- Security via biometrics, Spaced Domain based biometric and recognition techniques; Correlation based biometric filters, Basic theory of Correlation filters; Design of advanced correlation filters that offer tolerance to expected impairments; Methods to implement digital correlations; Applications of correlation filters

ISEA 208 Auditing, Securing standards and Best Practices

Course Content


ISEA 209 Web/Network/Wireless Penetration testing

Course Content

Web Application Security

- Web Application Security Lab
• HTTP Basics – Understanding Web technologies, Life cycle of HTTP Requests, Web Application Architectures and
• Introduction to Web Security – Authentication and authorization vulnerabilities
• Introduction to Web Application Common Vulnerabilities and Mitigation
• Web Security Configurations – METHODS, Directory permissions,
• File uploads, Error Handling, Tracking default applications and locking admin consoles,
• Testing SSL Servers, Session based vulnerabilities, URL Redirection and Data Exposure,
• Various Web vulnerabilities auditing and penetration testing

Penetration Testing (Web, Network & Wireless) & Malware Analysis
• Introduction to Web server Applications
• Introduction to Web Application attacks (SQL Injection, cross-site scripting and request forgery)
• Introduction to database security, Application Security, WWW Security
• Web server hardening.
• Introduction to wireless architecture, WLAN, Wireless Adhoc Networks
• Introduction to Wireless Standards and Technologies(802.11, Bluetooth)
• Introduction on Malwares, Behavior Analysis
• Introduction to Trojan, IRC boot Sample, Static Analysis.
• Introduction to Security Products
• Troubleshooting Web servers and clients

Vulnerability Analysis, Attacks & Management
• Introduction to Information Security Auditing/Penetration Testing
• Foot printing and Reconnaissance and Scanning Networks
• Testing and penetrating devices
• Enumeration of Devices
• Sniffing, Password Cracking Techniques and Dos/DDos Techniques

ISEA 2010 Introduction to Malware Reverse Engineering technologies and Methodologies

Course Content
• Tools & Techniques for “Run-Time” Analysis
• Crash-Course in x86 Assembly
• Basic Static Analysis
• Network Traffic Analysis
• Debugging & Disassembling Malicious Binaries

*******
Information Security Modules – Management or Advanced Modules

ISEA 301 Network Defense and Countermeasures (NDC)
Course Content
- Security Fundamentals – Firewalls, Types of Firewalls, Limitations of firewall, Intrusion Detection And Prevention, Intrusion risks, Security policy, Monitoring and reporting of traffics, Traffic shaping, Investigating and verifying detected intrusions, Recovering from, reporting and documenting intrusions, Define the Types of intrusion Prevention Systems, Intrusion prevention system basics, Limitations of Intrusion Prevention System, Spoof Prevention, DoS, QoS Policy, Web Application Firewall, Packet Signature and Analysis, Virtual Private Networks, Deploy and managing VPN, VPN Performance tuning and error handling, VPN routing, DMZ and virtual host, Reverse proxy

ISEA 302 Firewalls and IDS
Course Content
- Firewall design principles, Types of firewalls, Security policy, VPN, Packet filtering, Personal Firewall
- IDS and types of IDS, Log analysis, Security
- Infrastructure, PKI, VPN, E-Commerce security, Security Audits, Asset classification and Risk Analysis, Audit Trail, Reporting

ISEA 303 Cyber Forensics & Cyber Laws
Course Content
- Cyber Forensics
  - Introduction to Cyber Crime and Cyber Forensics, Basic Forensic Principles, Network Forensics, Mobile Device Forensics, Memory Forensics, General Computing Principles, Search and Seizure of Computers, Forensic Imaging & Verification, Data Recovery and Analysis, Investigative Techniques
- Cyber Law
- Lab Session with Case Studies

ISEA 304 Switching and Router Security
Course Content
- Introduction to the Router – User Interface, Router IOS, Connecting to a Router, Bringing up a Router, Setup Mode, Command-Line Interface, Logging into the Router, Overview of Router Modes, CLI Prompts, Basic commands

Layer 2 Switching – Switching basics, Configuring Switches, Setting the Passwords, Setting the Hostname, Setting IP Information, Configuring Interface Descriptions, Erasing the Switch Configuration

Virtual LANs (VLANs) VLAN Basics, Broadcast Control, Security, Flexibility and Scalability, VLAN Memberships, Static VLANs, Dynamic VLANs, Identifying VLANs, Frame Tagging, LAN Identification Methods, Inter-Switch Link (ISL) Protocol, Routing between VLANs, Configuring VLANs, Assigning Switch Ports to VLANs, Configuring Trunk Ports, Configuring Inter-VLAN Routing, VLAN Trunking Protocol (VTP), VTP Modes of Operation, VTP Pruning, Configuring VTP.


Network address translation NAT, Introduction to Network addresses Translation (NAT), Port address translation (PAT), Static NAT, Dynamic NAT, NAT Overloading

WAN Protocols: Introduction of WAN, Cabling the WAN, HDLC, PPP, LCP, Frame Relay, ISDN, DSL/ADSL.

ISEA 305 Ethical Hacking

Course Content

Ethical Hacking


- Malware Reverse Engineering

- Overview of Malware Reverse Engineering, Types of Malware, Malicious code Families, Latest Trends in Malware, Analysis of Malware

ISEA 306 Advanced security Management in Cloud computing with Virtualization

Course Content

Virtualization Basics

- Introduction to Virtualization, Virtualization Tools, Xen Virtualization, KVM Virtualization

Cloud Computing with SaaS & PaaS Deployment

- Introduction to Cloud Computing, Types of Cloud Services, Introduction to SaaS Cloud, SaaS Cloud Deployment with Open Source Tools, Introduction to PaaS Cloud, PaaS Cloud Server Deployment with Google App Engine/Aneka

- Advanced Cloud Infrastructure

(2 Weeks)
Introduction to IaaS Cloud, Types of Cloud Deployment with Xen/KVM, Setting Private Cloud with Windows, Setting Private Cloud with OpenStack, Deployment with Public Cloud

### ISEA 307 Data Center management & Security Administration and Security Operations

**Course Content**


### ISEA 308 Business Continuity and Disaster Recovery Planning

**Course Content**

- Information Technology Risk Identification & Assessment, Risk Response and Mitigation, Risk and Control Monitoring and Reporting.
- Overview of threat modeling process (Identity assets, create an architecture overview, Decompose the application, identify the threats, document the threats)
- Vulnerability classifications according to the assets class ( hardware, software, network, site and organization)

### ISEA 309 Security over Internet of Things

**Course Content**

- Lab session with case studies

### ISEA 3010 Security Analytics for Big Data

**Course Content**

- Introduction to Big Data Analytics – Big Data Overview, State of the Practice in Analytics, the Data Scientist, Big Data Analytics in Industry Verticals.
• Data Analytics Lifecycle – Discovery, Data Preparation, Model Planning, Model Building, Communicating Results, Operationalizing
• Advanced Analytics – Theory And Methods, K Means Clustering, Association Rules, Linear Regression, Logistic Regression, Naïve Bayesian Classifier, Decision Trees, Time Series Analysis, Text Analysis
• Advanced Analytics – Technologies and Tools, Analytics for Unstructured Data
  ✓ MapReduce and Hadoop, The Hadoop Ecosystem
  ⚡ In-database Analytics – SQL Essentials
  ⚡ Advanced SQL and MADlib for In-database Analytics
• The Endgame, or putting it All Together – Operationalizing an Analytics Project, Creating the Final Deliverables, Data Visualization Techniques, Final Lab Exercise on Big Data Analytics

*******