ACADEMIC REGULATIONS
COURSE STRUCTURE
AND
DETAILED SYLLABUS

M.TECH
CYBER FORENSIC & INFORMATION SECURITY / CYBER SECURITY

(Applicable for the batches admitted from 2013-14)

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD
KUKATPALLY, HYDERABAD – 500 085.

ACADEMIC REGULATIONS R13 FOR M. TECH. (REGULAR) DEGREE COURSE

Applicable for the students of M. Tech. (Regular) Course from the Academic Year 2013-14 and onwards

The M. Tech. Degree of Jawaharlal Nehru Technological University Hyderabad shall be conferred on candidates who are admitted to the program and who fulfil all the requirements for the award of the Degree.

1.0 ELIGIBILITY FOR ADMISSIONS

Admission to the above program shall be made subject to eligibility, qualification and specialization as prescribed by the University from time to time.

Admissions shall be made on the basis of merit/rank obtained by the candidates at the qualifying Entrance Test conducted by the University or on the basis of any other order of merit as approved by the University, subject to reservations as laid down by the Govt. from time to time.

2.0 AWARD OF M. TECH. DEGREE

2.1 A student shall be declared eligible for the award of the M. Tech. Degree, if he pursues a course of study in not less than two and not more than four academic years. However, he is permitted to write the examinations for two more years after four academic years of course work.

2.2 A student, who fails to fulfill all the academic requirements for the award of the degree within four academic years from the year of his admission, shall forfeit his seat in M. Tech. course.

2.3 The student shall register for all 88 credits and secure all the 88 credits.

2.4 The minimum instruction days in each semester are 90.

3.0 A. COURSES OF STUDY

The following specializations are offered at present for the M. Tech. course of study.

1. Advanced Manufacturing Systems
2. Aerospace Engineering/ Aeronautical Engineering
3. Automation
4. Biomedical Signal Processing and Instrumentation
5. Bio-Technology
6. CAD/CAM
7. Chemical Engineering
8. Communication Systems
9. Computer Networks
10. Computer Networks and Information Security
11. Computer Science
12. Computer Science and Engineering
13. Computers and Communication Engineering.
14. Construction Management
15. Control Engineering
16. Control Systems
17. Cyber Forensic / Cyber Security & Information Technology
18. Design for Manufacturing/ Design and Manufacturing
19. Digital Electronics and Communication Engineering.
20. Digital Electronics and Communication Systems
21. Digital Systems and Computer Electronics
22. Electrical Power Engineering
23. Electrical Power Systems
24. Electronics & Instrumentation

25. Electronics and Communication Engineering
26. Embedded Systems
27. Embedded Systems and VLSI Design
28. Energy Systems
29. Engineering Design
30. Environmental Engineering
31. Geoinformatics and Surveying Technology
32. Geotechnical Engineering.
33. Heating Ventilation & Air Conditioning.
34. Highway Engineering
35. Image Processing
36. Industrial Engineering and Management
37. Information Technology
38. Infrastructure Engineering
39. Machine Design
40. Mechatronics.
41. Microwave & Radar Engineering
42. Nano Technology
43. Neural Networks
44. Parallel Computing
45. Power and Industrial Drives
46. Power Electronics
47. Power Electronics and Electrical Drives
48. Power Engineering and Energy Systems
49. Power Plant Engineering & Energy Management
50. Power System Control and Automation
51. Power System with Emphasis H.V. Engineering / H.V. Engineering
52. Production Engineering.
53. Real Time Systems
54. Software Engineering
55. Structural Engineering
56. Systems & Signal Processing
57. Thermal Engineering.
58. Transportation Engineering
59. VLSI
60. VLSI and Embedded System/ Electronics Design Technology
61. VLSI Design
62. VLSI System Design
63. Web Technologies
64. Wireless and Mobile Communication

and any other course as approved by the University from time to time.

3.0 B. Departments offering M. Tech. Programmes with specializations are noted below:

Civil Engg.	Construction Management Environmental Engineering Geoinformatics and Surveying Technology Geotechnical Engineering Highway Engineering Infrastructure Engineering Structural Engineering Transportation Engineering
EEE	Control Engineering Control Systems Electrical Power Engineering Electrical Power Systems Power and Industrial Drives Power Electronics Power Electronics and Electrical Drives Power Engineering and Energy Systems Power Plant Engineering & Energy Management Power System Control and Automation Power System with Emphasis H.V. Engineering / H.V. Engineering
ME	Advanced Manufacturing Systems Automation CAD/CAM Design for Manufacturing/ Design and Manufacturing Energy Systems Engineering Design Heating Ventilation & Air Conditioning Industrial Engineering and Management Machine Design Mechatronics. Power Plant Engineering & Energy Management Production Engineering Thermal Engineering.
ECE	Biomedical Signal Processing and Instrumentation Communication Systems Computers and Communication Engineering. Digital Electronics and Communication Engineering. Digital Electronics and Communication Systems Digital Systems and Computer Electronics Electronics & Instrumentation Electronics and Communication Engineering Embedded Systems Embedded Systems and VLSI Design

	Microwave & Radar Engineering Systems & Signal Processing VLSI VLSI and Embedded System/ Electronics Design Technology VLSI Design VLSI System Design Wireless and Mobile Communication
CSE	Computer Networks Computer Networks and Information Security Computer Science Computer Science and Engineering Cyber Forensic / Cyber Security & Information Technology Image Processing Information Technology Neural Networks Parallel Computing Real Time Systems Software Engineering Web Technologies
Aeronautical Engg.	Aerospace Engineering / Aeronautical Engineering
Bio-technology	Bio-Technology
Chemical Engg.	Chemical Engineering
Nano Technology	Nano Technology

4.0 ATTENDANCE

The programs are offered on a unit basis with each subject being considered a unit.

4.1 A student shall be eligible to write University examinations if he acquires a minimum of 75% of attendance in aggregate of all the subjects.

4.2 Condonation of shortage of attendance in aggregate up to 10% (65% and above and below 75%) in each semester shall be granted by the College Academic Committee.

4.3 Shortage of Attendance below 65% in aggregate shall not be condoned.

4.4 Students whose shortage of attendance is not condoned in any semester are not eligible to write their end semester examination of that class and their registration shall stand cancelled.

4.5 A prescribed fee shall be payable towards condonation of shortage of attendance.

4.6 A student shall not be promoted to the next semester unless he satisfies the attendance requirement of the present semester, as applicable. They may seek readmission into that semester when offered next. If any candidate fulfills the attendance requirement in the present semester, he shall not be eligible for readmission into the same class.

4.7 A candidate shall put in a minimum required attendance at least in three (3) theory subjects in the present semester to get promoted to the next semester. In order to qualify for the award of the M. Tech. Degree, the candidate shall complete all the academic requirements of the subjects, as per the course structure.

4.8 A student shall not be promoted to the next semester unless he satisfies the attendance requirements of the previous semester including the days of attendance in sports, games, NCC and NSS activities.

5.0 EVALUATION

The performance of the candidate in each semester shall be evaluated subject-wise, with a maximum of 100 marks for theory and 100 marks for practicals, on the basis of Internal Evaluation and End Semester Examination.

5.1 For the theory subjects 60 marks shall be awarded based on the performance in the End Semester Examination and 40 marks shall be awarded based on the Internal Evaluation. The internal evaluation shall be made based on the average of the marks secured in the two Mid Term-Examinations conducted-one in the middle of the Semester and the other immediately after the completion of instruction. Each mid term examination shall be conducted for a total duration of 120 minutes with Part A as compulsory question (16 marks) which consists of four sub-questions and carries 4 marks each and Part B with 3 questions to be answered out of 5 questions each question for 8 marks. If any candidate is absent from any subject of a mid-term examination, an on-line test will be conducted for him by the University. The details of the Question Paper pattern for End Examination (Theory) is given below:

- The End semesters Examination will be conducted for 60 marks which consists of two parts viz. i).Part-A for 20 marks, ii). Part –B for 40 marks.
- Part-A is compulsory question where it consists of five questions one from each unit and carries four marks each. This will be treated as Question 1.
- Part-B consists of five Questions (numbered from 2 to 6) carries 8 marks each. Each of these questions is from one unit and may contain sub-questions. For each question there will be an "either" "or" choice (that means there will be two questions from each unit and the student should answer only one question)

5.2 For practical subjects, 60 marks shall be awarded based on the performance in the End Semester Examinations and 40 marks shall be awarded based on the day-to-day performance as Internal Marks.

5.3 There shall be two seminar presentations during I year I semester and II semester. For seminar, a student under the supervision of a faculty member, shall collect the literature on a topic and critically review the literature and submit it to the department in a report form and shall make an oral presentation before the Departmental Academic Committee consisting of Head of the Department, Supervisor and two other senior faculty members of the department. For each Seminar there will be only internal evaluation of 50 marks. A candidate has to secure a minimum of 50% of marks to be declared successful.

5.4 There shall be a Comprehensive Viva-Voce in II year I Semester. The Comprehensive Viva-Voce will be conducted by a Committee consisting of Head of the Department and two Senior Faculty members of the Department. The Comprehensive Viva-Voce is intended to assess the students' understanding of various subjects he has studied during the M. Tech. course of study. The Comprehensive Viva-Voce is evaluated for 100 marks by the Committee. There are no internal marks for the Comprehensive Viva-Voce.

5.5 A candidate shall be deemed to have secured the minimum academic requirement in a subject if he secures a minimum of 40% of marks in the End semester Examination and a minimum aggregate of 50% of the total marks in the End Semester Examination and Internal Evaluation taken together.

5.6 In case the candidate does not secure the minimum academic requirement in any subject (as specified in 5.5) he has to reappear for the End semester Examination in that subject. A candidate shall be given one chance to re-register for each subject provided the internal marks secured by a candidate are less than 50% and so has failed in the end examination. In such a case, the candidate must re-register for the subject(s) and secure the required minimum attendance. The candidate's attendance in the re-registered subject(s) shall be calculated separately to decide upon his eligibility for writing the end examination in those subject(s). In the event of the student taking another chance, his internal marks and end examination marks obtained in the previous attempt stand cancelled.

5.7 In case the candidate secures less than the required attendance in any subject, he shall not be permitted to write the End Examination in that subject. He shall re-register the subject when next

offered.

5.8 Laboratory examination for M. Tech. courses must be conducted with two Examiners, one of them being the Laboratory Class Teacher and the second examiner shall be another Laboratory Teacher.

6.0 EVALUATION OF PROJECT/DISSERTATION WORK

Every candidate shall be required to submit a thesis or dissertation on a topic approved by the Project Review Committee.

6.1 A Project Review Committee (PRC) shall be constituted with Principal as Chairperson, Heads of all the Departments offering the M. Tech. programs and two other senior faculty members.

6.2 Registration of Project Work: A candidate is permitted to register for the project work after satisfying the attendance requirement of all the subjects, both theory and practical.

6.3 After satisfying 6.2, a candidate has to submit, in consultation with his project supervisor, the title, objective and plan of action of his project work to the Departmental Academic Committee for approval. Only after obtaining the approval of the Departmental Academic Committee can the student initiate the Project work.

6.4 If a candidate wishes to change his supervisor or topic of the project, he can do so with the approval of the Departmental Academic Committee. However, the Departmental Academic Committee shall examine whether or not the change of topic/supervisor leads to a major change of his initial plans of project proposal. If yes, his date of registration for the project work starts from the date of change of Supervisor or topic as the case may be.

6.5 A candidate shall submit his status report in a bound-form in two stages at least with a gap of 3 months between them.

6.6 The work on the project shall be initiated at the beginning of the II year and the duration of the project is two semesters. A candidate is permitted to submit Project Thesis only after successful completion of theory and practical course with the approval of PRC not earlier than 40 weeks from the date of registration of the project work. For the approval of PRC the candidate shall submit the draft copy of thesis to the Principal through Head of the Department and make an oral presentation before the PRC.

6.7 Three copies of the Project Thesis certified by the supervisor shall be submitted to the College/ School/Institute.

6.8 The thesis shall be adjudicated by one examiner selected by the University. For this, the Principal of the College shall submit a panel of 5 examiners, eminent in that field, with the help of the guide concerned and head of the department.

6.9 If the report of the examiner is not favourable, the candidate shall revise and resubmit the Thesis, in the time frame as decided by the PRC. If the report of the examiner is unfavourable again, the thesis shall be summarily rejected.

6.10 If the report of the examiner is favourable, Viva-Voce examination shall be conducted by a board consisting of the Supervisor, Head of the Department and the examiner who adjudicated the Thesis. The Board shall jointly report the candidate's work as one of the following:

A. Excellent

B. Good

C. Satisfactory

D. Unsatisfactory

The Head of the Department shall coordinate and make arrangements for the conduct of Viva- Voce examination.

If the report of the Viva-Voce is unsatisfactory, the candidate shall retake the Viva-Voce examination only after three months. If he fails to get a satisfactory report at the second Viva- Voce examination, he will not be eligible for the award of the degree.

7.0 AWARD OF DEGREE AND CLASS

After a student has satisfied the requirements prescribed for the completion of the program and is eligible for the award of M. Tech. Degree he shall be placed in one of the following four classes:

Class Awarded	% of marks to be secured
First Class with Distinction	70% and above
First Class	Below 70% but not less than 60%
Second Class	Below 60% but not less than 50%
Pass Class	Below 50% but not less than 40%

The marks in internal evaluation and end examination shall be shown separately in the memorandum of marks.

8.0 WITHHOLDING OF RESULTS

If the student has not paid the dues, if any, to the university or if any case of indiscipline is pending against him, the result of the student will be withheld and he will not be allowed into the next semester. His degree will be withheld in such cases.

9.0 TRANSITORY REGULATIONS

9.1 Discontinued, detained, or failed candidates are eligible for admission to two earlier or equivalent subjects at a time as and when offered.

9.2 The candidate who fails in any subject will be given two chances to pass the same subject; otherwise, he has to identify an equivalent subject as per R13 academic regulations.

10. GENERAL

10.1 Wherever the words “he”, “him”, “his”, occur in the regulations, they include “she”, “her”, “hers”.

10.2 The academic regulation should be read as a whole for the purpose of any interpretation.

10.3 In the case of any doubt or ambiguity in the interpretation of the above rules, the decision of the Vice-Chancellor is final.

10.4 The University may change or amend the academic regulations or syllabi at any time and the changes or amendments made shall be applicable to all the students with effect from the dates notified by the University.

MALPRACTICES RULES

DISCIPLINARY ACTION FOR / IMPROPER CONDUCT IN EXAMINATIONS

	Nature of Malpractices/Improper conduct	Punishment
	If the candidate:	
1. (a)	Possesses or keeps accessible in examination hall, any paper, note book, programmable calculators, Cell phones, pager, palm computers or any other form of material concerned with or related to the subject of the examination (theory or practical) in which he is appearing but has not made use of (material shall include any marks on the body of the candidate which can be used as an aid in the subject of the examination)	Expulsion from the examination hall and cancellation of the performance in that subject only.
(b)	Gives assistance or guidance or receives it from any other candidate orally or by any other body language methods or communicates through cell phones with any candidate or persons in or outside the exam hall in respect of any matter.	Expulsion from the examination hall and cancellation of the performance in that subject only of all the candidates involved. In case of an outsider, he will be handed over to the police and a case is registered against him.
2.	Has copied in the examination hall from any paper, book, programmable calculators, palm computers or any other form of material relevant to the subject of the examination (theory or practical) in which the candidate is appearing.	Expulsion from the examination hall and cancellation of the performance in that subject and all other subjects the candidate has already appeared including practical examinations and project work and shall not be permitted to appear for the remaining examinations of the subjects of that Semester/ year. The Hall Ticket of the candidate is to be cancelled and sent to the University.
3.	Impersonates any other candidate in connection with the examination.	The candidate who has impersonated shall be expelled from examination hall. The candidate is also debarred and forfeits the seat. The performance of the original candidate who has been impersonated, shall be cancelled in all the subjects of the examination (including practicals and project work) already appeared and shall not be allowed to appear for examinations of the remaining subjects of that semester/year. The candidate is also debarred for two consecutive semesters from class work and all University examinations. The continuation of the course by the candidate is subject to the academic regulations in connection with forfeiture of seat. If the imposter is an outsider, he will be handed over to the police and a case is registered against him.

4.	Smuggles in the Answer book or additional sheet or takes out or arranges to send out the question paper during the examination or answer book or additional sheet, during or after the examination.	Expulsion from the examination hall and cancellation of performance in that subject and all the other subjects the candidate has already appeared including practical examinations and project work and shall not be permitted for the remaining examinations of the subjects of that semester/year. The candidate is also debarred for two consecutive semesters from class work and all University examinations. The continuation of the course by the candidate is subject to the academic regulations in connection with forfeiture of seat.
5.	Uses objectionable, abusive or offensive language in the answer paper or in letters to the examiners or writes to the examiner requesting him to award pass marks.	Cancellation of the performance in that subject.
6.	Refuses to obey the orders of the Chief Superintendent/Assistant – Superintendent / any officer on duty or misbehaves or creates disturbance of any kind in and around the examination hall or organizes a walk out or instigates others to walk out, or threatens the officer-in charge or any person on duty in or outside the examination hall of any injury to his person or to any of his relations whether by words, either spoken or written or by signs or by visible representation, assaults the officer-in-charge, or any person on duty in or outside the examination hall or any of his relations, or indulges in any other act of misconduct or mischief which result in damage to or destruction of property in the examination hall or any part of the College campus or engages in any other act which in the opinion of the officer on duty amounts to use of unfair means or misconduct or has the tendency to disrupt the orderly conduct of the examination.	In case of students of the college, they shall be expelled from examination halls and cancellation of their performance in that subject and all other subjects the candidate(s) has (have) already appeared and shall not be permitted to appear for the remaining examinations of the subjects of that semester/year. The candidates also are debarred and forfeit their seats. In case of outsiders, they will be handed over to the police and a police case is registered against them.
7.	Leaves the exam hall taking away answer script or intentionally tears of the script or any part thereof inside or outside the examination hall.	Expulsion from the examination hall and cancellation of performance in that subject and all the other subjects the candidate has already appeared including practical examinations and project work and shall not be permitted for the remaining examinations of the subjects of that semester/year. The candidate is also debarred for two consecutive semesters from class work and all University examinations. The continuation of the course by the candidate is subject to the academic regulations in connection with forfeiture of seat.

8.	Possess any lethal weapon or firearm in the examination hall.	Expulsion from the examination hall and cancellation of the performance in that subject and all other subjects the candidate has already appeared including practical examinations and project work and shall not be permitted for the remaining examinations of the subjects of that semester/year. The candidate is also debarred and forfeits the seat.
9.	If student of the college, who is not a candidate for the particular examination or any person not connected with the college indulges in any malpractice or improper conduct mentioned in clause 6 to 8.	Student of the colleges expulsion from the examination hall and cancellation of the performance in that subject and all other subjects the candidate has already appeared including practical examinations and project work and shall not be permitted for the remaining examinations of the subjects of that semester/year. The candidate is also debarred and forfeits the seat. Person(s) who do not belong to the College will be handed over to police and, a police case will be registered against them.
10.	Comes in a drunken condition to the examination hall.	Expulsion from the examination hall and cancellation of the performance in that subject and all other subjects the candidate has already appeared including practical examinations and project work and shall not be permitted for the remaining examinations of the subjects of that semester/year.
11.	Copying detected on the basis of internal evidence, such as, during valuation or during special scrutiny.	Cancellation of the performance in that subject and all other subjects the candidate has appeared including practical examinations and project work of that semester/year examinations.
12.	If any malpractice is detected which is not covered in the above clauses 1 to 11 shall be reported to the University for further action to award suitable punishment.	

Malpractices identified by squad or special invigilators

1. Punishments to the candidates as per the above guidelines.
2. Punishment for institutions : (if the squad reports that the college is also involved in encouraging malpractices)
   - (i) A show cause notice shall be issued to the college.
   - (ii) Impose a suitable fine on the college.
   - (iii) Shifting the examination centre from the college to another college for a specific period of not less than one year.

***

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD.

M.TECH - CYBER FORENSIC & INFORMATION SECURITY / CYBER SECURITY

COURSE STRUCTURE AND SYLLABUS

I Year I Semester

Code	Group	Subject	L	P	Credits
		Mathematical Foundation for Cyber Security	3	-	3
		Applied Cryptography	3	-	3
		Network and Wireless Security	3	-	3
		Biometric Systems and Biometric Image Processing	3	-	3
	Elective -I	Distributed and Cloud Computing Information Storage Management Information Systems Audit	3	-	3
	Elective -II	IT Security Metrics Web Security Distributed Systems	3	-	3
	Lab	Applied Cryptography Lab	-	3	2
		Seminar	-	-	2
		Total Credits	18	3	22

I Year II Semester

Code	Group	Subject	L	P	Credits
		Software Vulnerability Analysis	3	-	3
		Intrusion Detection and Prevention Systems	3	-	3
		Cyber Crime Investigations and Digital Forensics	3	-	3
		Cyber Laws and Security Policies	3	-	3
	Elective -III	Information Theory and Coding Security Threats Digital Watermarking and Steganography	3	-	3
	Elective -IV	Network Programming Distributed Systems Security Intellectual Property Rights	3	-	3
	Lab	Ethical Hacking Lab	-	3	2
		Seminar	-	-	2
		Total Credits	18	3	22

II Year - I Semester

Code	Group	Subject	L	P	Credits
		Comprehensive Viva	-	-	2
		Project Seminar	-	3	2
		Project work	-	-	18
		Total Credits	-	3	22

II Year - II Semester

Code	Group	Subject	L	P	Credits
		Project work and Seminar	-	-	22
		Total Credits	-	-	22

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

M. Tech – I Year – I Sem. (CF&IS/Cyber Security)

MATHEMATICAL FOUNDATIONS FOR CYBER SECURITY

Unit- I

Number Theory: Introduction - Divisibility - Greatest common divisor - Prime numbers - Fundamental theorem of arithmetic - Mersenne primes - Fermat numbers - Euclidean algorithm - Fermat's theorem - Euler totient function - Euler's theoerem. Congruences: Definition - Basic properties of congruences - Residue classes - Chinese remainder theorem.

Unit- II

Algebraic Structures: Groups – Cyclic groups, Cosets, Modulo groups - Primitive roots - Discrete logarithms. Rings – Sub rings, ideals and quotient rings, Integral domains. Fields – Finite fields – GF (p^n), GF(2^n) - Classification - Structure of finite fields. Lattice, Lattice as Algebraic system, sub lattices, some special lattices. .

Unit -III

Probability Theory: Introduction – Concepts of Probability - Conditional Probability - Baye's Theorem - Random Variables – discrete and continuous- central Limit Theorem-Stochastic Process- Markov Chain.

Unit -IV

Coding Theory: Introduction - Basic concepts: codes, minimum distance, equivalence of codes, Linear codes - Linear codes - Generator matrices and parity-check matrices - Syndrome decoding – Hamming codes - Hadamard Code - Goppa codes.

Unit -V

Pseudorandom Number Generation: Introduction and examples - Indistinguishability of Probability Distributions - Next Bit Predictors - The Blum-Blum-Shub Generator – Security of the BBS Generator.

REFERENCES:

1. Ivan Niven, Herbert S. Zuckerman, and Hugh L. Montgomery, 'An introduction to the theory of numbers', John Wiley and Sons 2004.
2. Douglas Stinson, 'Cryptography – Theory and Practice', CRC Press, 2006.
3. Sheldon M Ross, "Introduction to Probability Models", Academic Press, 2003.
4. C.L. Liu, 'Elements of Discrete mathematics', McGraw Hill, 2008.
5. Fraleigh J. B., 'A first course in abstract algebra', Narosa, 1990.
6. Joseph A. Gallian, ''Contemporary Abstract Algebra', Narosa, 1998.

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

M. Tech – I Year – I Sem. (CF&IS/Cyber Security)

APPLIED CRYPTOGRAPHY

Unit-I

Foundations – Protocol Building Blocks - Basic Protocols - Intermediate Protocols - Advanced Protocols - Zero-Knowledge Proofs - Zero-Knowledge Proofs of Identity -Blind Signatures - Identity-Based Public-Key Cryptography - Oblivious Transfer - Oblivious Signatures - Esoteric Protocols.

Unit-II

Key Length - Key Management - Electronic Codebook Mode - Block Replay - Cipher Block Chaining Mode - Stream Ciphers - Self-Synchronizing Stream Ciphers - Cipher-Feedback Mode - Synchronous Stream Ciphers - Output-Feedback Mode - Counter Mode - Choosing a Cipher Mode - Interleaving - Block Ciphers versus Stream Ciphers - Choosing an Algorithm - PublicKey Cryptography versus Symmetric Cryptography - Encrypting Communications Channels - Encrypting Data for Storage - Hardware Encryption versus Software Encryption - Compression, Encoding, and Encryption - Detecting Encryption – Hiding and Destroying Information.

Unit- III

Information Theory - Complexity Theory - Number Theory - Factoring - Prime Number Generation - Discrete Logarithms in a Finite Field - Data Encryption Standard (DES) – Lucifer -Madryga - NewDES - GOST – 3 Way – Crab – RC5 - Double Encryption - Triple Encryption - CDMF Key Shortening - Whitening.

Unit- IV

Pseudo-Random-Sequence Generators and Stream Ciphers – RC4 - SEAL - Feedback with Carry Shift Registers - Stream Ciphers Using FCSRs - Nonlinear-Feedback Shift Registers - System-Theoretic Approach to Stream-Cipher Design - Complexity-Theoretic Approach to Stream-Cipher Design - N- Hash - MD4 - MD5 - MD2 - Secure Hash Algorithm (SHA) - OneWay Hash Functions Using Symmetric Block Algorithms - Using Public-Key Algorithms - Message Authentication Codes.

Unit- V

RSA - Pohlig-Hellman - McEliece - Elliptic Curve Cryptosystems -Digital Signature Algorithm (DSA) - Gost Digital Signature Algorithm - Discrete Logarithm Signature Schemes - Ongchnorr-Shamir -Cellular Automata - Feige-Fiat-Shamir -Guillou-Quisquater - Diffie-Hellman - Station-to-Station Protocol -Shamir's Three-Pass Protocol - IBM Secret-Key Management Protocol - MITRENET - Kerberos - IBM Common Cryptographic Architecture.

(subject may be taught with implementation through JAVA)

REFERENCES

1. Bruce Schneier, "Applied Cryptography: Protocols, Algorithms, and Source Code in C" John Wiley & Sons, Inc, 2nd Edition, 1996.
2. Wenbo Mao, "Modern Cryptography Theory and Practice", Pearson Education, 2004
3. Atul Kahate, "Cryptography and Network Security", Tata McGrew Hill, 2003.
4. William Stallings, "Cryptography and Network Security, Prentice Hall, New Delhi, 2006.
5 Bernard Menezes, "Network Security and Cryptography", Cengage Learning, New Delhi, 2010.

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

M. Tech – I Year – I Sem. (CF&IS/Cyber Security)

NETWORK AND WIRELESS SECURITY

Unit- I

Introduction: Network concepts – Threats in networks – Network security controls – Importance of security – Threat models – Security concepts – Common mitigation methods.

Authentication: Overview of authentication – Authentication of people – Security Handshake pitfalls – Strong password protocols – Kerberos – Public key infrastructure.

IP & Web Security: IP security: Overview - Architecture – Authentication Header - Encapsulating Security Payload - Key management – Web security: Web security considerations – Secure Socket Layer and Transport Layer Security – Secure electronic transaction – Web issues.

Electronic Mail Security: Store and forward – Security services for e-mail – Establishing keys – Privacy – Authentication of the Source – Message Integrity – Non-repudiation – Proof of submission and delivery - Pretty Good Privacy – Secure/Multipurpose Internet Mail Extension.

Unit- II

WIRELESS TECHNOLOGIES: Introduction to wireless technologies- Wireless data networks-Personal Area Networks -Transmission Media – WLAN standards - Securing WLANS - Countermeasures - WEP (Wired Equivalence Protocol).

Wireless Threats: - Kinds of security breaches - Eavesdropping - Communication Jamming - RF interference - Covert wireless channels - DOS attack – Spoofing - Theft of services - Traffic Analysis - Cryptographic threats - Wireless security Standards.

Unit- III

Security in Data Networks: Wireless Device security issues - CDPD security (Cellular Digital Packet Data)-GPRS security (General Packet Radio Service) - GSM (Global System for Mobile Communication) security – IP security.

Unit -IV

Wireless Transport Layer Security: Secure Socket Layer - Wireless Transport Layer Security - WAP Security Architecture - WAP Gateway.

Unit -V

Bluetooth Security: Basic specifications – Piconets – Bluetooth security architecture – Scatternets – Security at the baseband layer and link layer – Frequency hopping – Security manager – Authentication – Encryption – Threats to Bluetooth security.

REFERENCES:

1. Charles P. Fleeger, “Security in Computing”, Prentice Hall, New Delhi, 2009.
2. Behrouz A.Forouzan, “Cryptography & Network Security”, Tata McGraw Hill, India, New Delhi, 2009.
3. William Stallings, “Cryptography and Network Security, Prentice Hall, New Delhi, 2006.
4. Bruce Schneier, “Applied Cryptography”, John Wiley & Sons, New York, 2004.
5. Nichols and Lekka, “Wireless Security-Models, Threats and Solutions”, Tata McGraw – Hill, New Delhi, 2006.
6. Merritt Maxim and David Pollino, ”Wireless Security”, Osborne/McGraw Hill, New Delhi, 2005.

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

M. Tech – I Year – I Sem. (CF&IS/Cyber Security)

BIOMETRIC SYSTEMS AND BIOMETRIC IMAGE PROCESSING

Objectives:

This course introduces the basic biometric system, classification and applications. The student will be introduced the fundamentals of biometric technologies, basic techniques in image processing for fingerprint and iris based identification.

Unit -I:

Introduction: Biometric fundamentals – Biometric technologies – Biometrics Vs traditional techniques – Characteristics of a good biometric system – Benefits of biometrics – Key biometric processes: verification, identification and biometric matching – Performance measures in biometric systems, FAR, FRR, FTE rate, EER and ATV rate, Applications of Biometric Systems, Security and Privacy Issues.

Physiological Biometrics : Leading technologies : Finger-scan – Facial-scan – Iris-scan – Voice-scan – components, working principles, competing technologies, strengths and weaknesses – Other physiological biometrics : Hand-scan, Retina-scan –components, working principles, competing technologies, strengths and weaknesses – Automated fingerprint identification systems.

Unit- II:

Behavioral Biometrics: Leading technologies: Signature-scan – Keystroke scan – components, working principles, strengths and weaknesses.

Privacy and Standards in Biometrics: Assessing the Privacy Risks of Biometrics – Designing Privacy-Sympathetic Biometric Systems – Need for standards – different biometric standards.

Unit- III:

Fundamentals of Image Processing: Digital Image representation - Fundamental steps in Image Processing Image Enhancement: The Spatial Domain Methods, The Frequency Domain Methods - Image Segmentation: Pixel Classification by Thresholding, Histogram Techniques, Smoothing and Thresholding - Gradient Based Segmentation: Gradient Image, Boundary Tracking, Laplacian Edge Detection.

Unit -IV:

Fingerprint Biometrics: Fingerprint Patterns, Fingerprint Features, Fingerprint Image, width between two ridges - Fingerprint Image Processing - Minutiae Determination - Fingerprint Matching: Fingerprint Classification, Matching policies.

Unit- V:

Iris Biometrics: Iris System Architecture, Definitions and Notations - Iris Recognition: Iris location, Doubly Dimensionless Projection, Iris code, Comparison - Coordinate System: Head Tilting Problem, Basic Eye Model, Searching Algorithm, Texture Energy Feature.

References for Biometric systems:

1. Anil K Jain, Patrick Flynn, Arun A Ross, “Handbook of Biometrics”, Springer, 2008.
2. Anil K Jain, Arun A Ross, Karthik Nandakumar, “Introduction to Biometrics”, Springer, 2011.
3. Samir Nanavati, Michael Thieme, Raj Nanavati, “Biometrics – Identity Verification in a Networked World”, Wiley-dreamtech India Pvt Ltd, New Delhi, 2003.
4. Paul Reid, “Biometrics for Network Security”, Pearson Education, New Delhi, 2004.
5. John R Vacca, “Biometric Technologies and Verification Systems”, Elsevier Inc, 2007.

References for Biometric Image processing:

1. David D. Zhang, “Automated Biometrics: Technologies and Systems”, Kluwer Academic Publishers, New Delhi, 2000.
2. Rafael C.Gonzalez, Richard E.Woods, Steven L.Eddins, “Digital Image Processing”, Pearson Education, New Delhi, 2009.
3. Arun A. Ross , Karthik Nandakumar, A.K.Jain, “Handbook of Multibiometrics”, Springer, New Delhi, 2006.

Outcome :

After the completion of the course, the student should be able to Understand different biometric technologies, applications and classification, Security issues etc. Understand image processing techniques for fingerprint and iris based identification.

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

M. Tech – I Year – I Sem. (CF&IS/Cyber Security)

DISTRIBUTED AND CLOUD COMPUTING

(Elective-I)

Unit-I

Systems Modeling, Clustering and Virtualization

Distributed System Models and Enabling Technologies, Computer Clusters for Scalable Parallel Computing, Virtual Machines and Virtualization of Clusters and Data centers.

Unit-II

Foundations: Introduction to Cloud Computing, Migrating into a Cloud, Enriching the 'Integration as a Service' Paradigm for the Cloud Era, The Enterprise Cloud Computing Paradigm.

Unit-III

Infrastructure as a Service (IAAS) & Platform and Software as a Service (PAAS / SAAS)

Virtual machines provisioning and Migration services, On the Management of Virtual machines for Cloud Infrastructures, Enhancing Cloud Computing Environments using a cluster as a Service, Secure Distributed Data Storage in Cloud Computing.

Aneka, Comet Cloud, T-Systems', Workflow Engine for Clouds, Understanding Scientific Applications for Cloud Environments.

Unit-IV

Monitoring, Management and Applications

An Architecture for Federated Cloud Computing, SLA Management in Cloud Computing, Performance Prediction for HPC on Clouds, Best Practices in Architecting Cloud Applications in the AWS cloud, Building Content Delivery networks using Clouds, Resource Cloud Mashups.

Unit-V

Governance and Case Studies: Organizational Readiness and Change management in the Cloud age, Data Security in the Cloud, Legal Issues in Cloud computing, Achieving Production Readiness for Cloud Services.

TEXT BOOKS:

1. Cloud Computing: Principles and Paradigms by Rajkumar Buyya, James Broberg and Andrzej M. Goscinski, Wiley, 2011.
2. Distributed and Cloud Computing, Kai Hwang, Geoffery C.Fox, Jack J.Dongarra, Elsevier, 2012.

REFERENCE BOOKS:

1. Cloud Computing : A Practical Approach, Anthony T.Velte, Toby J.Velte, Robert Elsenpeter, Tata McGraw Hill, rp2011.
2. Enterprise Cloud Computing, Gautam Shroff, Cambridge University Press, 2010.
3. Cloud Computing: Implementation, Management and Security, John W. Rittinghouse, James F.Ransome, CRC Press, rp2012.
4. Cloud Application Architectures: Building Applications and Infrastructure in the Cloud, George Reese, O'Reilly, SPD, rp2011.
5. Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance, Tim Mather, Subra Kumaraswamy, Shahed Latif, O'Reilly, SPD, rp2011.

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

M. Tech – I Year – I Sem. (CF&IS/Cyber Security)

INFORMATION STORAGE MANAGEMENT

(Elective-I)

Unit-I

Introduction to Storage Technology: Data proliferation and the varying value of data with time & usage, Sources of data and states of data creation, Data center requirements and evolution to accommodate storage needs, Overview of basic storage management skills and activities, The five pillars of technology, Overview of storage infrastructure components, Evolution of storage, Information Lifecycle Management concept, Data categorization within an enterprise, Storage and Regulations.

Unit-II

Storage Systems Architecture: Intelligent disk subsystems overview, Contrast of integrated vs. modular arrays, Component architecture of intelligent disk subsystems, Disk physical structure- components, properties, performance, and specifications, Logical partitioning of disks, RAID & parity algorithms, hot sparing, Physical vs. logical disk organization, protection, and back end management, Array caching properties and algorithms, Front end connectivity and queuing properties, Front end to host storage provisioning, mapping, and operation, Interaction of file systems with storage, Storage system connectivity protocols.

Unit-III

Introduction to Networked Storage: JBOD, DAS, SAN, NAS, & CAS evolution, Direct Attached Storage (DAS) environments: elements, connectivity, & management, Storage Area Networks (SAN): elements & connectivity, Fibre Channel principles, standards, & network management principles, SAN management principles, Network Attached Storage (NAS): elements, connectivity options, connectivity protocols (NFS, CIFS, ftp), & management principles, IP SAN elements, standards (iSCSI, FCIP, iFCP), connectivity principles, security, and management principles, Content Addressable Storage (CAS): elements, connectivity options, standards, and management principles, Hybrid Storage - solutions overview including technologies like virtualization & appliances.

Unit-IV

Introductions to Information Availability: Business Continuity and Disaster Recovery Basics, Local business continuity techniques, Remote business continuity techniques, Disaster Recovery principles & techniques.

Managing & Monitoring: Management philosophies (holistic vs. system & component), Industry management standards (SNMP, SMI-S, CIM), Standard framework applications, Key management metrics (thresholds, availability, capacity, security, performance), Metric analysis methodologies & trend analysis, Reactive and pro-active management best practices, Provisioning & configuration change planning, Problem reporting, prioritization, and handling techniques, Management tools overview.

Unit-V

Securing Storage and Storage Virtualization: Define storage security. , List the critical security attributes for information systems, describe the elements of a shared storage model and security extensions, Define storage security domains, List and analyze the common threats in each domain, Identify different virtualization technologies, describe block-level and file level virtualization technologies and processes.

REFERENCES

1. Marc Farley Osborne, “Building Storage Networks”, Tata Mac Graw Hill, 2001.
2. Robert Spalding and Robert Spalding, “Storage Networks: The Complete Reference”, Tata McGraw Hill, 2003.
3. Meeta Gupta, “Storage Area Network Fundamentals”, Pearson Education Ltd., 2002.
4. Gerald J Kowalski and Mark T Maybury,” Information Storage Retreival Systems theory & Implementation”, BS Publications, 2000.
5. Thejendra BS, “Disaster Recovery & Business continuity”, Shroff Publishers & Distributors, 2006.

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

M. Tech – I Year – I Sem. (CF&IS/Cyber Security)

INFORMATION SYSTEMS AUDIT

(Elective-I)

Unit- I

Overview of Information System Auditing, Effect of Computers on Internal Controls, Effects of Computers on Auditing, Foundations of information Systems Auditing, Conducting an Information Systems Audit.

The management Control Framework-I: Introduction, Evaluating the planning Function, Evaluating the Leading Function, Evaluating the Controlling Function, Systems Development Management Controls, Approaches to Auditing Systems Development, Normative Models of the Systems Development Process, Evaluating the Major phases in the Systems Development Process, Programming Management Controls, Data Resource Management Controls.

Unit- II

The Management Control Framework-II: Security Management Controls, Operations management Controls Quality assurance Management Controls.

The Application Control Framework-I: Boundary Controls, Input Controls, Communication Controls.

Unit-III

The Application Control Framework-II: Processing Controls, Database Controls, output Controls.

Unit- IV

Evidence Collection: Audit Software, Code Review, Test Data, and Code Comparison, Concurrent Auditing techniques, Interviews, Questionnaires, and Control Flowcharts. Performance Management tools.

Unit -V

Evidence Evaluation: Evaluating Asset Safeguarding and Data Integrity, Evaluating System Effectiveness, Evaluating System Efficiency.

References

1. Ron Weber, Information Systems Control and Audit, Pearson Education, 2002.
2. M.Revathy Sriram, Systems Audit, TMH, New Delhi, 2001.
3. Jalote : Software Project Mangement in Practice, Pearson Education.
4. Royce : Software Project Management, Pearson Education.

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

M. Tech – I Year – I Sem. (CF&IS/Cyber Security)

IT SECURITY METRICS

(Elective-II)

Unit-I:

What Is a **Security Metric?** Metric and Measurement, Security Metrics Today, The Dissatisfying State of Security Metrics, Reassessing Our Ideas About Security Metrics. **Designing Effective Security Metrics:** Choosing Good Metrics, GQM for Better Security Metrics, More Security Uses for GQM, Summary.

Unit-II:

Understanding Data: What are Data? Data Sources for Security Metrics; We Have Metrics and Data - Now what, Summary, Case Study 1. **The Security Process Management** Framework: Managing Security as a Business Process, the SPM Framework, Before You Begin SPM, Summary. **The Analyzing Security Metrics Data:** The Most Important Step, Analysis Tools and Techniques, Summary. **Designing the Security Measurement Project:** Before the Project Begins, Phase One: Build a Project Plan and Assemble the Team, Phase two: Gather the Metrics Data, phase Three: Analyze the Metrics Data and Build Conclusions, phase Four: Present Results, Phase Five: Reuse the Results, Project Management Tools, Summary.

Unit-III:

Measurements **Security Operations:** Sample Metrics for Security Operations, Sample Measurement Project for Security Operations, Summary. **Measuring Compliance and Conformance:** The Challenges of Measuring Compliance, Sample Measurement Projects for Compliance and Conformance, Summary.

Unit-IV:

Measuring Security Cost and Value: Sample Measurement Projects for Compliance and Conformance, The Importance of Data to Measuring Cost and Value, Summary. **Measuring People, Organizations, and Culture:** Sample Measurement Projects for People, Organizations, and Culture, Summary.

Unit-V:

The Security Improvement Program: Moving from Projects to Programs, Managing Security Measurement with a Security, Requirements for a SIP, Measuring the SIP. Summary. **Learning Security: Different Contexts for Security Process Management:** Organizational Learning, Three Learning Styles for IT Security Metrics, Final Thoughts, Summary.

Text Books:

1. IT SECURITY METRICS, Lance Hayden, TATA McGraw-HILL.
2. SECURITY METRICS, CAROLINE WONG, TATA McGraw-HILL.

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

M. Tech – I Year – I Sem. (CF&IS/Cyber Security)

WEB SECURITY

(Elective-II)

Unit-I

Introduction- A web security forensic lesson, Web languages, Introduction to different web attacks. Overview of N-tier web applications, Web Servers: Apache, IIS, Database Servers.

Unit-II

Review of computer security, Public Key cryptography, RSA. Review of Cryptography Basics, On-line Shopping, Payment Gateways.

Unit-III

Web Hacking Basics HTTP & HTTPS URL, Web Under the Cover Overview of Java security Reading the HTML source, Applet Security Servlets Security Symmetric and Asymmetric Encryptions, Network security Basics, Firewalls & IDS.

Unit-IV

Digital Certificates, Hashing, Message Digest, & Digital Signatures.

Unit-V

Basics, Securing databases, Secure JDBC, Securing Large Applications, Cyber Graffiti.

Text Books:

1. McClure, Stuart, Saumil Shah, and Shreeraj Shah. Web Hacking:attacks and defense. Addison Wesley. 2003.
2. Garms, Jess and Daniel Somerfield. Professional Java Security. Wrox. 2001.

Related Web Sites:

1. Collection of Cryptography Web Sites, Publications, FAQs, and References: http://world.std.com/~franl/crypto.html.
2. FAQ: What is TLS/SSL? http://www.mail.nih.gov/user/faq/tlsssl.htm.
3. The Open SSL Project (SDKs for free download): http://www.openssl.org/.
4. Windows & .NET security updates Web site: http://www.ntsecurity.net/.

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

M. Tech – I Year – I Sem. (CF&IS/Cyber Security)

DISTRIBUTED SYSTEMS

(Elective-II)

Unit-I

Characterization of Distributed Systems. Design Issues, User Requirement, Network Technologies and Protocols, IPC, Client-Server Communication, Group Communication, IPC in UNIX.

Remote Procedure Calling, Design issues, Implementation, Asynchronous RPC

Unit-II

Distributed OS, Its kernel, Processes and Threads, Naming and Protection, Communication and Invocation, Virtual Memory, File Service components, Design issues, Interfaces, implementation techniques, SUN network file systems

Unit-III

SNS – a name service model, its design issues, Synchronizing physical clocks, Logical time and logical clocks, Distributed coordination. Replication and its architectural model, Consistency and request ordering, Conversation between a client and a server, Transactions, Nested Transactions.

Unit-IV

Concurrency control Locks, Optimistic concurrency control, Timestamp ordering, Comparison of methods for concurrency control.

Distributed Transactions and Nested Transactions, Atomic commit protocols, Concurrency control in distributed transactions, distributed Deadlocks, Transactions with replicated data, Transaction recovery, Fault tolerance, Hierarchical and group masking of faults.

Unit-V

Cryptography, Authentication and key distribution, Logics of Authentication, Digital signatures.

Distributed shared memory, Design and Implementation issues, Sequential consistency and ivy, Release consistency and Munin, Overview of Distributed Operating systems Mach, Chorus.

Text Book:

1. G Coulouris, J Dollimore and T Kindberg - Distributed Systems Concepts and Design, Third Edition, Pearson Education.

Reference Books:

1. M Singhal, N G Shivarathri - Advanced Concepts in Operating Systems, Tata McGraw Hill Edition.
2. A.S. Tanenbaum and M.V. Steen - Distributed Systems – Principles and Paradigms, Pearson education.

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

M. Tech – I Year – I Sem. (CF&IS/Cyber Security)

APPLIED CRYPTOGRAPHY LAB

1. Implementation of symmetric cipher algorithm(AES and RC4).
2. Random number generation using a subset of digits and alphabets.
3. Implementation of RSA based signature system.
4. Implementation of Subset sum.
5. Authenticating the given signature using MD5 hash algorithm.
6. Implementation of Diffie-Hellman algorithm.
7. Implementation EIGAMAL cryptosystem.
8. Implementation of Goldwasser-Micali probabilistic public key system.
9. Implementation of Rabin Cryptosystem. (Optional).
10. Implementation of Kerberos cryptosystem.
11. Firewall implementation and testing.
12. Implementation of a trusted secure web transaction.
13. Cryptographic Libraries-Sun JCE/Open SSL/Bouncy Castle JCE.
14. Digital Certificates and Hybrid (ASSY/SY) encryption, PKI.
15. Message Authentication Codes.
16. Elliptic Curve cryptosystems (Optional).
17. PKCS Standards (PKCS1, 5, 11, 12), Cipher modes.

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

M. Tech – I Year – II Sem. (CF&IS/Cyber Security)

SOFTWARE VULNERABILITY ANALYSIS

Unit-I:

Introduction to security & Authentication: Software Security **-** Dealing with Widespread Security Failures, Bugtraq, CERT Advisories, RISKS Digest,Technical Trends Affecting Software Security, The 'iliities, Beyond Reliability, Penetrate and Patch, an Art and Engineering, Security Goals, Prevention, Traceability and Auditing, Monitoring, Privacy and Confidentiality, Multilevel Security, Anonimity, Authentication, Integrity, Know Your Enemy – Common Software Security Pitfalls. Software Project Goals.

Unit-II:

Application Security & Malicious Code: Managing Software Security Risk: An overview of Software Risk Management For Security, The Role of Security Personnel, Software Security Personnel in the Life Cycle, Deriving Requirements, Risk Assessment, Design For Security, Implementation and Testing, A Dose Of Reality, Getting People To Think About Security, Software Risk Management In Practice, When Development Goes Astray, Code Review (Tools) - Architectural Risk Analysis - Penetration Testing - Risk-Based Security Testing - Abuse Cases - Security Requirements - Security Operations.

Unit-III:

Access Control & Physical Protection: The UNIX Access Control Model, How UNIX Permissions Work? Modifying File Attributes, Modifying Ownership, The umask, The Programmatic Interface, Setuid Programming, Access Control In Windows NT, Compartmentalization, Fine-Grained Privileges.Buffer Overflow & Rootkits: Buffer Overflows As Security Problems, Defending Against Buffer Overflow, Major Gotchas, Internal Buffer Overflows, More Input Overflows, Other Risks, Tools for handling buffer overflows, Smashing Heaps And Stacks, Heap Overflows, Stack Overflows, Decodong The Stack, To Infinity … And Beyond!, Attack Code, A UNIX Exploit, What About Windows?

Unit-IV:

Network Security & Intrusion: Brief Review of OSI Model, Sockets, Socket Functions, Socket Addresses, Network Byte Order, Internet Address Conversion, Simple Server and Web Clients, Tinyweb Server. Peeling Back the Lower Layers - Data-Link Layer - Network Layer- Transport Layer - Network Sniffing - Raw Socket Sniffer - libpcap Sniffer - Decoding the Layers - Active Sniffing - Denial of Service - SYN Flooding - The Ping of Death - Teardrop - Ping Flooding - Amplification Attacks - Distributed DoS Flooding - TCP/IP Hijacking - RST Hijacking - Continued Hijacking - Port Scanning - Stealth SYN Scan - FIN, X-mas, and Null Scans - Spoofing Decoys - Idle Scanning - Proactive Defense (shroud) - Reach Out and Hack Someone - Analysis with GDB - Almost Only Counts with Hand Grenades - Port-Binding Shellcode.

Unit-V:

Counter Measures: Detection of System Daemons, Crash Course in Signals, Tinyweb Daemon, Tools of the Trade, tinywebd Exploit Tool, Log Files, Blend In with the Crowd, Overlooking the Obvious, One Step at a Time, Putting Things Back Together Again, Child Laborers, Advanced Camouflage, Spoofing the Logged IP Address, Logless Exploitation, The Whole Infrastructure, Socket Reuse, Payload Smuggling, String Encoding, How to Hide a Sled, Buffer Restrictions, Polymorphic Printable ASCII Shellcode. Hardening Countermeasures - Nonexecutable Stack, ret2libc,Returning into system(). Randomized Stack Space - Investigations with BASH and GDB, Bouncing Off linux-gate. Applied Knowledge, First Attempts, Paying the Odds.

Text Books:

1. John Viega & Gary McGraw: Building Secure Software: How to Avoid Security Problems the Right Way (Addison-Wesley Professional Computing Series) [Paperback].
2. Gary McGraw: Software Security: Building Security In (Addison-Wesley Professional Computing Series) [Paperback].

Reference Books :

1. Michael Howard, David LeBlanc, John Viega: 19 Deadly Sins of Software Security: Programming Flaws and How to Fix Them (Security One-off) (Addison-Wesley Professional Computing Series) [Paperback].
2. Jon Erickson: Hacking: The Art of Exploitation, 2nd Edition (No Starch Press, San Fransico) [Paperback].
3. Richard Sinn " Software Security , Theory Programming and Practice" Cengage Learning.

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

M. Tech – I Year – II Sem. (CF&IS/Cyber Security)

INTRUSION DETECTION AND PREVENTION SYSTEMS

Unit-I

Introduction: Understanding Intrusion Detection – Intrusion detection and prevention basics – IDS and IPS analysis schemes, Attacks, Detection approaches –Misuse detection – anamoly detection – specification based detection – hybrid detection.

Theoretical Foundations of Detection: Taxonomy of anomaly detection system – fuzzy logic – Bayes theory – Artificial Neural networks – Support vector machine – Evolutionary computation – Association rules – Clustering.

Unit-II

Architecture and Implementation: Centralized – Distributed – Cooperative Intrusion Detection - Tiered architecture.

Unit-III

Justifying Intrusion Detection: Intrusion detection in security – Threat Briefing – Quantifying risk – Return on Investment (ROI).

Unit-IV

Applications and Tools: Tool Selection and Acquisition Process - Bro Intrusion Detection – Prelude Intrusion Detection - Cisco Security IDS - Snorts Intrusion Detection – NFR security.

Unit-V

legal issues and Organizations Standards: Law Enforcement / Criminal Prosecutions – Standard of Due Care – Evidentiary Issues, Organizations and Standardizations.

REFERENCES:

1. Ali A. Ghorbani, Wei Lu, “Network Intrusion Detection and Prevention: Concepts and Techniques”, Springer, 2010.
2. Carl Enrolf, Eugene Schultz, Jim Mellander, “Intrusion detection and Prevention”, McGraw Hill, 2004
3. Paul E. Proctor, “The Practical Intrusion Detection Handbook “,Prentice Hall , 2001.
4. Ankit Fadia and Mnu Zacharia, “Intrusiion Alert”, Vikas Publishing house Pvt., Ltd, 2007.
5. Earl Carter, Jonathan Hogue, “Intrusion Prevention Fundamentals”, Pearson Education, 2006.

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

M. Tech – I Year – II Sem. (CF&IS/Cyber Security)

CYBER CRIME INVESTIGATIONS AND DIGITAL FORENSICS

Unit -I

Introduction: Introduction and Overview of Cyber Crime, Nature and Scope of Cyber Crime, Types of Cyber Crime: Social Engineering, Categories of Cyber Crime, Property Cyber Crime.

Unit -II

Cyber Crime Issues: Unauthorized Access to Computers, Computer Intrusions, White collar Crimes, Viruses and Malicious Code, Internet Hacking and Cracking, Virus Attacks, Pornography, Software Piracy, Intellectual Property, Mail Bombs, Exploitation ,Stalking and Obscenity in Internet, Digital laws and legislation, Law Enforcement Roles and Responses.

Unit -III

Investigation: Introduction to Cyber Crime Investigation, Investigation Tools, eDiscovery, Digital Evidence Collection, Evidence Preservation, E-Mail Investigation, E-Mail Tracking, IP Tracking, E-Mail Recovery, Hands on Case Studies. Encryption and Decryption Methods, Search and Seizure of Computers, Recovering Deleted Evidences, Password Cracking.

Unit -IV

Digital Forensics: Introduction to Digital Forensics, Forensic Software and Hardware, Analysis and Advanced Tools, Forensic Technology and Practices, Forensic Ballistics and Photography, Face, Iris and Fingerprint Recognition, Audio Video Analysis, Windows System Forensics, Linux System Forensics, Network Forensics.

Unit -V

Laws and Acts: Laws and Ethics, Digital Evidence Controls, Evidence Handling Procedures, Basics of Indian Evidence ACT IPC and CrPC , Electronic Communication Privacy ACT, Legal Policies.

REFERENCES:

1. Nelson Phillips and Enfinger Steuart, “Computer Forensics and Investigations”, Cengage Learning, New Delhi, 2009.
2. Kevin Mandia, Chris Prosise, Matt Pepe, “Incident Response and Computer Forensics “, Tata McGraw -Hill, New Delhi, 2006.
3. Robert M Slade,” Software Forensics”, Tata McGraw - Hill, New Delhi, 2005.
4. Bernadette H Schell, Clemens Martin, “Cybercrime”, ABC – CLIO Inc, California, 2004.
5. ”Understanding Forensics in IT “, NIIT Ltd, 2005.

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

M. Tech – I Year – II Sem. (CF&IS/Cyber Security)

CYBER LAWS AND SECURITY POLICIES

Unit-I

Introduction to Computer Security: Definition, Threats to security, Government requirements, Information Protection and Access Controls, Computer security efforts, Standards, Computer Security mandates and legislation, Privacy considerations, International security activity.

Unit-II

Secure System Planning and administration, Introduction to the orange book, Security policy requirements, accountability, assurance and documentation requirements, Network Security, The Red book and Government network evaluations.

Unit-III

Information security policies and procedures: Corporate policies- Tier 1, Tier 2 and Tier3 policies - process management-planning and preparation-developing policies-asset classification policy-developing standards.

Unit- IV

Information security: fundamentals-Employee responsibilities- information classification- Information handling- Tools of information security- Information processing-secure program administration.

Unit-V

Organizational and Human Security: Adoption of Information Security Management Standards, Human Factors in Security- Role of information security professionals.

REFERENCES

1. Debby Russell and Sr. G.T Gangemi, “Computer Security Basics (Paperback)”, 2ndEdition, O’ Reilly Media, 2006.
2. Thomas R. Peltier, “Information Security policies and procedures: A Practitioner’s Reference”, 2nd Edition Prentice Hall, 2004.
3. Kenneth J. Knapp, “Cyber Security and Global Information Assurance: Threat Analysis and Response Solutions”, IGI Global, 2009.
4. Thomas R Peltier, Justin Peltier and John blackley, ”Information Security Fundamentals”, 2nd Edition, Prentice Hall, 1996.
5. Jonathan Rosenoer, “Cyber law: the Law of the Internet”, Springer-verlag, 1997.
6. James Graham, “ Cyber Security Essentials” Averbach Publication T & F Group.

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

M. Tech – I Year – II Sem. (CF&IS/Cyber Security)

INFORMATION THEORY AND CODING

(Elective-III)

UNIT -I

Random Variables and Processes: Events - Random variables - Distribution and density functions - Operations on random variables - Covariance - Correlation functions - Random process - Stationarity - Spectral decomposition - Response of linear system to random inputs, Relation between information and probability.

UNIT- II

Information Entropy Fundamentals: Self information measure - mutual and self information - Entropy function - Characteristics of Entropy function - Conditional Entropies - Derivation of the noise characteristics of a channel - Redundancy - Efficiency and channel capacity - capacities of channels with symmetric noise structure. Huffman coding: Implementation of Huffman code, Shannon's theorem, Code design, Shannon - Fano coding.

Unit-III

Error Control Coding : Backward error correction linear block codes, BCH codes, Golay codes, efficiency of LBC, forward correction codes-Convolution coding decoding algorithms, Viterbi decoding optimum decoding performance **measures.**

Unit- IV

Data and Voice Coding: Context dependent coding, arithmetic codes, overall efficiency consideration. Voice coding, Delta Modulation and adaptive delta modulation, linear predictive coding, silence coding, sub-band coding.

Unit -V

Compression Techniques: Principles – Text compression –Static Huffman Coding - Dynamic Huffman coding. Arithmetic coding – Image Compression – Graphics Interchange format – Tagged Image File Format – Digitized documents – Introduction to JPEG standards.

REFERENCES:

1. Reza F M, "An Introduction to Information Theory", McGraw Hill, 2000.
2. Viterbi A and Omura J K, "Principles of Digital Communication and Coding", McGraw Hill, 1979.
3. Cover T M and Thomas J A, "Elements of Information theory", 2nd edition, John Wiley & Sons, 2006.
4. Sheldon M Ross, "Introduction to Probability Models", Academic Press, 2003.
5. Roth R, "Introduction to Coding theory", Cambridge University Press, 2006.
6. Peter Sweeney, "Error Control Coding: From Theory to Practice", John Wiley & Sons, 2002.

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

M. Tech – I Year – II Sem. (CF&IS/Cyber Security)

SECURITY THREATS

(Elective-III)

Unit-I

Introduction: Security threats - Sources of security threats- Motives - Target Assets and vulnerabilities – Consequences of threats- E-mail threats - Web-threats - Intruders and Hackers, Insider threats, Cyber crimes.

Unit-II

Network Threats: Active/ Passive – Interference – Interception – Impersonation – Worms – Virus – Spam's – Ad ware - Spy ware – Trojans and covert channels – Backdoors – Bots - IP Spoofing - ARP spoofing - Session Hijacking - Sabotage-Internal treats- Environmental threats - Threats to Server security.

Unit-III

Security Threat Management: Risk Assessment - Forensic Analysis - Security threat correlation – Threat awareness - Vulnerability sources and assessment- Vulnerability assessment tools -Threat identification - Threat Analysis - Threat Modeling - Model for Information Security Planning.

Unit-IV

Security Elements: Authorization and Authentication - types, policies and techniques - Security certification - Security monitoring and Auditing - Security Requirements Specifications - Security Polices and Procedures, Firewalls, IDS, Log Files, Honey Pots.

Unit-V

Access control, Trusted Computing and multilevel security - Security models, Trusted Systems, Software security issues, Physical and infrastructure security, Human factors – Security awareness, training , Email and Internet use policies.

REFERENCES

1. Joseph M Kizza, "Computer Network Security", Springer Verlag, 2005.
2. Swiderski, Frank and Syndex, "Threat Modeling", Microsoft Press, 2004.
3. William Stallings and Lawrie Brown, "Computer Security: Principles and Practice", Prentice Hall, 2008.
4. Thomas Calabres and Tom Calabrese, "Information Security Intelligence: Cryptographic Principles & Application", Thomson Delmar Learning, 2004.

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

M. Tech – I Year – II Sem. (CF&IS/Cyber Security)

DIGITAL WATERMARKING AND STEGANOGRAPHY

(Elective-III)

UNIT I

Introduction: Information Hiding, Steganography and Watermarking – History of watermarking – Importance of digital watermarking – Applications – Properties – Evaluating watermarking systems

Watermarking Models & Message Coding: Notation – Communications – Communication based models – Geometric models – Mapping messages into message vectors – Error correction coding – Detecting multi-symbol watermarks.

UNIT II

Watermarking with Side Information & Analyzing Errors: Informed Embedding – Informed Coding – Structured dirty-paper codes - Message errors – False positive errors – False negative errors – ROC curves – Effect of whitening on error rates.

UNIT III

Perceptual Models: Evaluating perceptual impact – General form of a perceptual model – Examples of perceptual models – Robust watermarking approaches - Redundant Embedding, Spread Spectrum Coding, Embedding in Perceptually significant coefficients.

UNIT IV

Watermark Security & Authentication: Security requirements – Watermark security and cryptography – Attacks – Exact authentication – Selective authentication – Localization – Restoration.

UNIT V

Steganography: Steganography communication – Notation and terminology – Information-theoretic foundations of steganography – Practical steganographic methods – Minimizing the embedding impact – Steganalysis.

REFERENCES:

1. Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, Jessica Fridrich, Ton Kalker, “Digital Watermarking and Steganography”, Margan Kaufmann Publishers, New York, 2008.
2. Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, “Digital Watermarking”, Margan Kaufmann Publishers, New York, 2003.
3. Michael Arnold, Martin Schmucker, Stephen D. Wolthusen, “Techniques and Applications of Digital Watermarking and Contest Protection”, Artech House, London, 2003.
4. Juergen Seits, “Digital Watermarking for Digital Media”, IDEA Group Publisher, New York, 2005.
5. Peter Wayner, “Disappearing Cryptography – Information Hiding: Steganography & Watermarking”, Morgan Kaufmann Publishers, New York, 2002.

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

M. Tech – I Year – II Sem. (CF&IS/Cyber Security)

NETWORK PROGRAMMING

(Elective-IV)

UNIT-I

Introduction to Network Programming: OSI model, Unix standards, TCP and UDP & TCP connection establishment and Format, Buffer sizes and limitation, standard internet services, Protocol usage by common internet application.

Sockets : Address structures, value – result arguments, Byte ordering and manipulation function and related functions Elementary TCP sockets – Socket, connect, bind, listen, accept, fork and exec function, concurrent servers. Close function and related function.

UNIT-II

TCP client server: Introduction, TCP Echo server functions, Normal startup, terminate and signal handling server process termination, Crashing and Rebooting of server host shutdown of server host.

Elementary UDP sockets: Introduction UDP Echo server function, lost datagram, summary of UDP example, Lack of flow control with UDP, determining outgoing interface with UDP.

I/O Multiplexing: I/O Models, select function, Batch input, shutdown function, poll function, TCP Echo server.

UNIT-III

Socket Options: getsockopt and setsockopt functions. Socket states, Generic socket option IPV6 socket option ICMPV6 socket option IPV6 socket option and TCP socket options.

Advanced I/O Functions: Introduction, Socket Timeouts, recv and send Functions, readv and writev Functions, recvmsg and sendmsg Functions, Ancillary Data, How Much Data Is Queued? Sockets and Standard I/O, T/TCP: TCP for Transactions.

UNIT-IV

Elementary name and Address conversions: DNS, gethost by Name function, Resolver option, Function and IPV6 support, uname function, other networking information.

Daemon Processes and inetd Superserver – Introduction, syslogd Daemon, syslog Function, daemon_init Function, inetd Daemon, daemon_inetd Function.

Broadcasting- Introduction, Broadcast Addresses, Unicast versus Broadcast, dg_cli Function Using Broadcasting, Race Conditions.

Multicasting- Introduction, Multicast Addresses, Multicasting versus Broadcasting on A LAN, Multicasting on a WAN, Multicast Socket Options, mcast_join and Related Functions, dg_cli Function Using Multicasting, Receiving MBone Session Announcements, Sending and Receiving, SNTP: Simple Network Time Protocol, SNTP (Continued).

UNIT-V

Raw Sockets-Introduction, Raw Socket Creation, Raw Socket Output, Raw Socket Input, Ping Program, Traceroute Program, An ICMP Message Daemon.

Datalink Access- Introduction, BPF: BSD Packet Filter, DLPI: Data Link Provider Interface, Linux: SOCK_PACKET, libpcap: Packet Capture Library, Examining the UDP Checksum Field.

Remote Login: Terminal line disciplines, Pseudo-Terminals, Terminal modes, Control Terminals, rlogin Overview, RPC Transparency Issues.

Text Books:

1. UNIX Network Programming, by W. Richard Stevens, Bill Fenner, Andrew M. Rudoff, Pearson Education.
2. UNIX Network Programming, 1st Edition, - W.Richard Stevens. PHI.

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

M. Tech – I Year – II Sem. (CF&IS/Cyber Security)

DISTRIBUTED SYSTEMS SECURITY

(Elective-IV)

UNIT-I

Introduction – Distributed Systems, Distributed Systems Security. Security in Engineering: Secure Development Lifecycle Processes - A Typical Security Engineering Process – Security Engineering Guidelines and Resources. Common Security Issues and Technologies: Security Issues, Common Security Techniques.

UNIT-II

Host-level Threats and Vulnerabilities: Transient code Vulnerabilities - Resident Code Vulnerabilities - Malware: Trojan Horse – Spyware - Worms/Viruses – Eavesdropping – Job Faults. Infrastructure-Level Threats and Vulnerabilities: Network-Level Threats and Vulnerabilities - Grid Computing Threats and Vulnerabilities – Storage Threats and Vulnerabilities – Overview of Infrastructure Threats and Vulnerabilities.

UNIT-III

Application-Level Threats and Vulnerabilities: Application-Layer Vulnerabilities –Injection Vulnerabilities - Cross-Site Scripting (XSS) - Improper Session Management - Improper Error Handling - Improper Use of Cryptography - Insecure Configuration Issues - Denial of Service - Canonical Representation Flaws - Overflow Issues. Service-Level Threats and Vulnerabilities: SOA and Role of Standards - Service-Level Security Requirements - Service-Level Threats and Vulnerabilities - Service-Level Attacks - Services Threat Profile.

UNIT-IV

Host-Level Solutions: Sandboxing – Virtualization - Resource Management - Proof-Carrying Code -Memory Firewall – Antimalware. Infrastructure-Level Solutions: Network-Level Solutions - Grid-Level Solutions - Storage-Level Solutions. Application-Level Solutions: Application-Level Security Solutions.

UNIT-V

Service-Level Solutions: Services Security Policy - SOA Security Standards Stack – Standards in Dept - Deployment Architectures for SOA Security - Managing Service-Level Threats - Compliance in Financial Services - SOX Compliance - SOX Security Solutions – Multilevel Policy-Driven Solution Architecture - Case Study: Grid - The Financial Application – Security Requirements Analysis. Future Directions - Cloud Computing Security – Security Appliances - Usercentric Identity Management - Identity-Based Encryption (IBE) - Virtualization in Host Security.

REFERENCES :

1. Abhijit Belapurakar, Anirban Chakrabarti and et al., “Distributed Systems Security: Issues. Processes and solutions”, Wiley, Ltd., Publication, 2009.
2. Abhijit Belapurkar, Anirban Chakrabarti, Harigopal Ponnapalli, Niranjan Varadarajan, Srinivas Padmanabhuni and Srikanth Sundarrajan, “Distributed Systems Security: Issues, Processes and Solutions”, Wiley publications, 2009.
3. Rachid Guerraoui and Franck Petit, “Stabilization, Safety, and Security of Distributed Systems”, Springer, 2010.

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

M. Tech – I Year – II Sem. (CF&IS/Cyber Security)

INTELLECTUAL PROPERTY RIGHTS

(Elective-IV)

UNIT-I

Introduction to Intellectual Property Law – The Evolutionary Past - The IPR Tool Kit- Para -Legal Tasks in Intellectual Property Law Ethical obligations in Para Legal Tasks in Intellectual Property Law - Introduction to Cyber Law – Innovations and Inventions Trade related Intellectual Property Right.

UNIT-II

Introduction to Trade mark – Trade mark Registration Process – Post registration Procedures – Trade mark maintenance - Transfer of Rights - Inter partes Proceeding – Infringement - Dilution Ownership of Trade mark – Likelihood of confusion - Trademarks claims – Trademarks Litigations – International Trade mark Law.

UNIT-III

Introduction to Copyrights – Principles of Copyright Principles -The subjects Matter of Copy right – The Rights Afforded by Copyright Law – Copy right Ownership, Transfer and duration – Right to prepare Derivative works – Rights of Distribution – Rights of Perform the work Publicity Copyright Formalities and Registrations - Limitations - Copyright disputes and International Copyright Law – Semiconductor Chip Protection Act.

UNIT -IV

The law of patents-patent searches –Patent owner shp and transfer-Patent infringement-International Patent Law.

UNIT-V

Introduction to Trade Secret – Maintaining Trade Secret – Physical Security – Employee Limitation - Employee confidentiality agreement - Trade Secret Law - Unfair Competition – Trade Secret Litigation – Breach of Contract – Applying State Law.

BOOKS:

1. Debirag E.Bouchoux: "Intellectual Property". Cengage learning, New Delhi.
2. M.Ashok Kumar and Mohd.Iqbal Ali: "Intellectual Property Right" Serials Pub.
3. Cyber Law. Texts & Cases, South-Western's Special Topics Collections.
4. Prabhuddha Ganguli: ' Intellectual Property Rights" Tata Mc-Graw –Hill, New Delhi.
5. J Martin and C Turner "Intellectual Property" CRC Press.
6. Richard Stimm " Intellectual Property" Cengage Learning.

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

M. Tech – I Year – II Sem. (CF&IS/Cyber Security)

ETHICAL HACKING LAB (using Hacking Tools)

1. Footprinting.
2. Phishing.
3. Scanning Goal of DoS :dos attack(denial of services)- to reduce the speed of website:tool- http flooder.
4. Enumeration Session Hijacking.
5. System Hacking : man in the middle attack-:tool-etter cap (backtrack), cain abel (windows).
6. Network Level Hijacking.
7. Trojans and Backdoors RST Hijacking: trojans attack- to exploit an attack on computer system using IP Tools- Beast Server, Donald Dik, GirlFriend Attack(Reverse IP Attack).
8. Viruses and Worms (identification and removal using tools).
9. Hacking Web Servers: cpanel attack- for pruning control panel of web server/website: tool- brutas.
10. Web-Based Password Cracking Techniques: blind sql injection- to exploit website: tool- havij pro, sql map, the mole.
11. Hacking Wireless Networks: Email Tracker- to trace the route of any email or Ip: tool-Ip Locater,Email_Spidr,Aid4Mail.
12. Windows hacking- Windows Login Password Cracking Tool-NT Offline Password Cracking, ERD Commander, Loft_Crack, Kon_Boot.
13. software cracking/reverse engineering- finding key of particular software tools- odbg, code Fusion, resource hacker.
14. Wifi crack- to crack the keys of wifi tool- aircrack(linux) cain abel(windows), Lan Guard, Wireshark, BurpSuite.
15. Webshell hunter- to find if shell is uploaded in the website or not tool- X-code Xploit Scanner.

Some more tools for reference:

Metasploit Pro 4.5.0 - Penetration Testing Software.

WiFi Password Decryptor version 1.0 - Free Wireless account password cracking software

Nmap 6.25 - Free Security Scanner For Network Exploration & Security Audits.

PySQLi - Python framework to exploit complex SQL injection vulnerabilities.

BeEF - The Browser Exploitation Framework.

BeEF (Browser Exploitation Framework) is a powerful penetration testing tool that focuses on the web browser.

OWASP Joomscan -Joomla vulnerability scanner identifies 673 vulnerabilities.

SSLsplit: Tool for man-in-the-middle attacks against SSL/TLS encrypted network connections.

Secunia PSI 3.0 Released : Personal Software Inspector (PSI).

Burp Suite, a tool for performing security testing of web applications.

NinjaWPass for WordPress: protect WordPress login form against keyloggers and stolen passwords.

sqlmap: automatic SQL injection attack tool.