CURRICULUM AND DETAILED SYLLABI

FOR

M.E DEGREE (Computer Science and Information Security) PROGRAM

FOR THE STUDENTS ADMITTED FROM THE

ACADEMIC YEAR 2014-2015

THIAGARAJAR COLLEGE OF ENGINEERING
(A Government Aided ISO 9001-2000 certified
Autonomous Institution affiliated to AnnaUniversity)

MADURAI – 625 015, TAMILNADU

Phone: 0452 – 2482240, 41
Fax: 0452 2483427
Web: www.tce.edu

Approved in Board of Studies Meeting on 5.7.2014 Approved in Academic Council Meeting on 19.7.2014

Department of Information Technology

Graduating Students of M.E program of Computer Science and Information Security will be able to

1. Contribute effectively as an individual to serve the society through Information Security enabled solutions and products adhering to the ethics and principles.
2. Participate in interdisciplinary activities and provide novel engineering design and solutions by promoting research activities
3. Pursue life-long learning through self-learning and research by adapting to the dynamic technology changes
4. Demonstrate professionalism by acquiring different roles in Information Technology arena.

M.E. Computer Science and Information Security - ELIGIBILITY

Candidates for admission to the first semester of four semester M.E. (Computer Science and Information Security) should have passed B.E / B.Tech in Computer Science and Engineering / Information Technology through regular course of study from an AICTE approved institution or an examination of any University or authority accepted by the Anna University as equivalent thereto, with at least 55% marks in the degree examination or equivalent CGPA.

Scheduling of Courses

(For Students admitted in the Year 2014-2015)

Semester	Courses						Laboratory/ Project
4th (12)							**14IS410** Project **0:12**
3rd (16)	**14IS310** Information Security Program Development and Management **3:1**	**14ISPX0** Elective-IV **3:1**	**14ISPX0** Elective-V **3:1**				**14IS340** Project **0:4**
2nd (24)	**14IS210** Systems Security **3:1**	**14IS220** Data Analytics **3:0**	**14IS230** Cloud Security **3:1**	**14ISPX0** Elective-I **3:1**	**14ISPX0** Elective-II **3:1**	**14ISPX0** Elective-III **3:1**	**14IS270** Data Analytics Lab **0:1**
1st (24)	**14IS110** Graphs and Combinatorial Algorithms **3:0**	**14IS120** Cryptography **3:1**	**14IS130** Network Security **3:0**	**14IS140** Network Technologies **3:1**	**14IS150** Secure Software Engineering **3:1**	**14IS160** Database Security **3:1**	**14IS170** Cryptography and Network Security Lab **0:1**

CURRICULUM AND DETAILED SYLLABI

FOR

M.E DEGREE (Computer Science and Information Security) PROGRAM

FIRST SEMESTER

FOR THE STUDENTS ADMITTED FROM THE

ACADEMIC YEAR 2014-2015

THIAGARAJAR COLLEGE OF ENGINEERING
(A Government Aided ISO 9001-2000 certified
Autonomous Institution affiliated to AnnaUniversity)

MADURAI – 625 015, TAMILNADU

Phone: 0452 – 2482240, 41
Fax: 0452 2483427
Web: www.tce.edu

Approved in Board of Studies Meeting on 5.7.2014 Approved in Academic Council Meeting on 19.7.2014

THIAGARAJAR COLLEGE OF ENGINEERING: MADURAI – 625 015

(An Autonomous Institution Affiliated to Anna University)

CURRICULUM

(For the Students admitted from academic Year 2014-2015)

Name of the Degree: M.E (Computer Science and Information Security)

SUBJECTS OF STUDY

I SEMESTER

Theory

Subject code	Name of the subject	Regulation			
		L	T	P	C
14IS110	Graphs and Combinatorial Algorithms	3	1	0	4
14IS120	Cryptography	3	1	0	4
14IS130	Network Security	3	0	0	3
14IS140	Network Technologies	3	1	0	4
14IS150	Secure Software Engineering	3	1	0	4
14IS160	Database Security	3	1	0	4
Practical					
14IS170	Cryptography and Network Security Lab	0	0	3	1

Total Credits 24

II SEMESTER

Theory

Subject code	Name of the subject	Regulation			
		L	T	P	C
14IS210	Systems Security	3	1	0	4
14IS220	Data Analytics	3	0	0	3
14IS230	Cloud Security	3	1	0	4
14ISPX0	Elective-I	3	1	0	4
14ISPX0	Elective-II	3	1	0	4
14ISPX0	Elective-III	3	1	0	4
Practical					
14IS270	Data Analytics Lab	0	0	3	1

Total Credits 24

III SEMESTER
Theory:

Subject code	Name of the subject	Regulation			
		L	**T**	**P**	**C**
14IS310	Information Security Program Development and Management	3	1	0	4
14ISPX0	Elective-IV	3	1	0	4
14ISPX0	Elective-V	3	1	0	4
Practical:					
14IS340	Project	0	0	12	4

Total Credits 16

IV SEMESTER
Practical:

Subject code	Name of the subject	Regulation			
		L	**T**	**P**	**C**
14IS410	Project	3	1	0	4

Total Credits 12

Total No. of Credits to be earned for the award of degree: 76

List of Electives

1. Information Theory and Coding
2. Digital Watermarking and Steganography
3. Social Network Analysis
4. Web Mining
5. Machine Learning
6. Operating Sysyteem fundamentals and Security
7. Wireless Security
8. Formal Methods for Security
9. Big data technologies
10. Biometrics
11. Ethical Hacking and Cyber forensics
12. Information Security Governance
13. Information Risk Management and Compliance
14. Information Security Incident Management
15. Intrusion Detection and Prevention
16. Cyber Laws and Ethics
17. Information Retrieval
18. Cognitive Science

THIAGARAJAR COLLEGE OF ENGINEERING: MADURAI – 625 015

M.E Degree (Computer Science and Information Security) Program

SCHEME OF EXAMINATIONS

(For the candidates admitted from 2014-2015 onwards)

I SEMESTER

S.No.	Sub. code	Name of the subject	Duration of Terminal Exam. in Hrs.	Marks			Minimum Marks for Pass	
				Continuous Assessment *	Terminal Exam **	Max. Marks	Terminal Exam	Total
THEORY								
1	14IS110	Graphs and Combinatorial Algorithms	3	50	50	100	25	50
2	14IS120	Cryptography	3	50	50	100	25	50
3	14IS130	Network Security	3	50	50	100	25	50
4	14IS140	Network Technologies	3	50	50	100	25	50
5	14IS150	Secure Software Engineering	3	50	50	100	25	50
6	14IS160	Database Security	3	50	50	100	25	50
PRACTICAL								
7	14IS170	Cryptography and Network Security Lab	3	50	50	100	25	50

II SEMESTER

S.No.	Sub. code	Name of the subject	Duration of Terminal Exam. in Hrs.	Marks			Minimum Marks for Pass	
				Continuous Assessment *	Terminal Exam **	Max. Marks	Terminal Exam	Total
THEORY								
1	14IS210	Systems Security	3	50	50	100	25	50
2	14IS220	Data Analytics	3	50	50	100	25	50
3	14IS230	Cloud Security	3	50	50	100	25	50
4	14ISPX0	Elective-I	3	50	50	100	25	50
5	14ISPX0	Elective-II	3	50	50	100	25	50
6	14ISPX0	Elective-III	3	50	50	100	25	50
PRACTICAL								
7	14IS270	Cryptography and Cyber Forensics Lab	3	50	50	100	25	50

III SEMESTER

S.No.	Sub. code	Name of the subject	Duration of Terminal Exam. in Hrs.	Marks			Minimum Marks for Pass	
				Continuous Assessment *	Terminal Exam **	Max. Marks	Terminal Exam	Total
THEORY								
1	14IS310	Information Security Program Development and Management	3	50	50	100	25	50
2	14ISPX0	Elective-IV	3	50	50	100	25	50
3	14ISPX0	Elective-V	3	50	50	100	25	50
PRACTICAL								
4	14IS340	Project	-	150	150	300	75	150

IV Semester

S.No.	Sub. code	Name of the subject	Duration of Terminal Exam. in Hrs.	Marks			Minimum Marks for Pass	
				Continuous Assessment *	Terminal Exam **	Max. Marks	Terminal Exam	Total
PRACTICAL								
1	14IS410	Project	-	150	150	300	75	150

SubCode	Lectures	Tutorial	Practical	Credit
14IS110	3	1	-	4

14IS110 Graphs and Combinatorial Algorithms 3:1

Preamble: Combinatorial reasoning underlies all analysis of computer systems. Two of the most basic mathematical aspects of computer science concern the speed and logical structure. Speed involves enumeration of the number of times each step in a program can be performed. Logical structure involves flow charts, a form of graphs. In graph theory, combinatorial arguments are made a little easier by the use of pictures of the graphs. Natural form of graphs is sets with logical or hierarchical sequencing, such as computer flow charts. In case of network flows, we shall see that the flow optimization algorithm can also be used to prove several well-known combinatorial theorems. The general counting methods involve permutations and combinations. These methods are very useful in constructing computer programs and in mastering many theoretical topics of computer science. Recurrence relations are one of the simplest ways to solve counting problems. The methods for solving recurrence relations appeared originally in the development of the theory of difference equations, cousins of differential equations.

Competencies:

At the end of the course the student will be able to

1. Verify the pairs of graphs which are isomorphic.
2. Calculate the regions of the given plane graph.
3. Examine the graph whose adjacency matrix is given below to see if is connected.
4. Apply the Augmenting flow Algorithm and calculate the maximal flow for the given graph
5. Determine the number of arrangements and selections using the basic counting principles.
6. Determine the recurrence relation.
7. Determine the solutions of the recurrence relation.

Assessment Pattern

Sl.No.	Bloom's	Test I	Test II	Test III / End
1.	Remember	30	30	10
2.	Understand	0	0	20
3.	Apply	70	70	70
4.	Analyze	0	0	0
5.	Evaluate	0	0	0
6.	Create	0	0	0

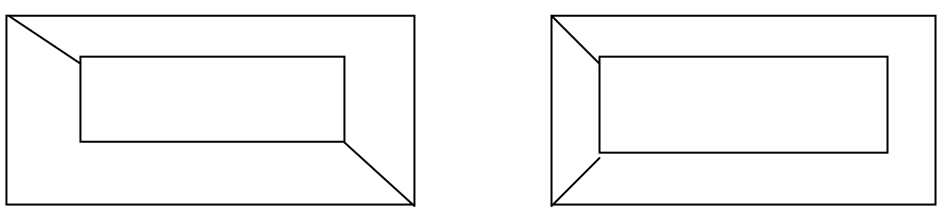
Course Level Learning Objectives

Remember

1. Define complete bipartite graph.
2. State Kruskal's algorithm.
3. Describe Edge- disjoint paths in a graph
4. State two basic counting principles.
5. Define recurrence relation.

Understand

1. State and prove Euler's formula.
2. Write the two algorithms for building a minimal spanning tree.
3. Explain Dijkstra's algorithms with an example
4. Write the Augmenting flow Algorithm and explain it.
5. Are the two graphs in the following figure isomorphic? Justify.



6. Explain Divide and Conquer relation in the analysis of recursive algorithms.

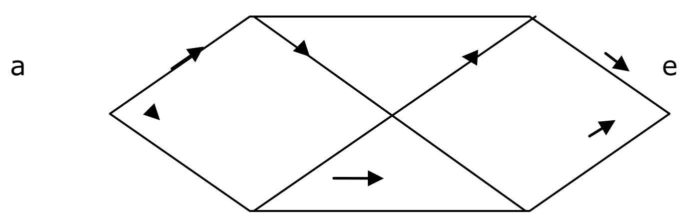
Apply

1. Show that an undirected graph has an Euler cycle if and only if it is connected and has all the vertices of even degree.
2. Examine the graph whose adjacency matrix is given below to see if is connected.

	X1	X2	X3	X4	X5	X6	X7	X8

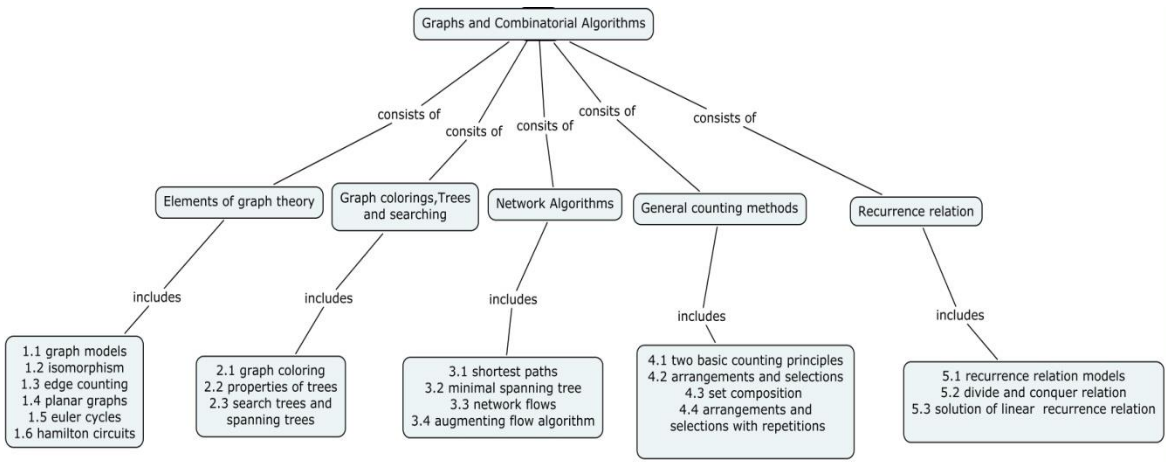
X1	0	1	1	1	0	1	0	0
X2	1	0	1	0	1	0	1	0
X3	1	1	0	0	0	0	0	0
X4	1	0	0	0	0	0	1	0
X5	0	1	0	0	0	0	1	0
X6	1	0	0	0	0	0	0	0
X7	0	1	0	1	1	0	0	1
X8	0	0	0	0	0	0	1	0

3. Apply the Augmenting flow Algorithm and calculate the maximal a - e flow for the graph given below.



4. What is the probability that a 4- digit campus telephone number has one or more repeated digits? And determine the probability that,
   i. (i). All 4 digits are the same.
   ii. (ii). 3 digits are the same, the other is different.
   iii. (ii). 2 digits are the same, the other 2 digits are each different.
5. Solve the recurrence relation $a_n = 2a_{n-1} + 3a_{n-2}$ with $a_0 = a_1 = 1$.
6. Determine how many ways are there to arrange the seven letter in the word SYSTEMS? In how many of these arrangements do the 3 S's appear consecutively?
7. Enumerate all arrangements of a, c, e, h in lexicographic order.

Concept map



Syllabus :Module-I: Elements of graph theory Graph models, isomorphism, Edge counting, Planar graphs, Euler cycles, Hamilton circuits. **Module-II: Coloring, trees and searching** Graph coloring, Chromatic polynomial, Properties of Trees, Cayley's theorem, Depth first and breadth first search, Spanning Trees**.** **Module-III: Network Algorithms**Shortest paths Algorithms , Minimal spanning trees, Network flows , Augmenting flow Algorithm, Max flow- Min cut theorem, Undirected networks-flow networks with supplies and demands . **Module-IV: Counting principles** Two basic counting principles , Simple Arrangements and selections, Set composition principle, Arrangements and selections with Repetitions , Generating permutation and combinations. **Module-V: Recurrence Relations** Recurrence Relations Models, Fibonacci number, Divide and conquer Relations, Solution of linear Recurrence Relations, Solution of in Homogeneous Recurrence Relations.

References:

1. Alan Thucker, "Applied Combinatories" , John Wiley and Sons, Inc, New York, Third Edition,1995.

2. CL Lin, " Introduction to Combinatorial Mathematics", Mcgraw Hill Book Company, New York, 1968.

3. Richard A.Brualdi, "Introductory Combinatories", North Holland, New York

Course Contents and Lecture schedule

S.No	**Topics**	**No. of Lectures**
	Module I Elements of graph theory (9)	
1	Review of the concepts of Set theory, relations & functions	1
2	Graph models, Isomorphism	2
3	Edge counting	1

4	Planar graphs	2
5	Euler cycles	1
6	Hamilton circuits	1
7	Tutorial	1
	Module-II Coloring , trees and searching(10)	
8	Graph coloring	2
9	Chromatic polynomial	1
10	Properties of Trees	2
11	Cayley's theorem	1
12	Depth first and breadth first search	2
13	Spanning Trees	1
14	Tutorial	1
	Module-III Network Algorithms(7)	
15	Shortest paths Algorithms	1
16	Minimal spanning trees	1
17	Network flows	1
18	Augmenting flow Algorithms	1
19	Max flow- Min cut theorem	1
20	Undirected networks-flow networks with supplies and demands	1
21	Tutorial	1
	Module-IV Counting principles(6)	
22	Two basic counting principles	1
23	Simple Arrangements and selections	1
24	Set composition principle	1
25	Arrangements and selections with Repetitions	1
26	Generating permutation and combinations	1
27	Tutorial	1
	Module-V Recurrence Relations(8)	
28	Recurrence Relations Models	1
29	Fibonacci number	1
30	Divide and conquer Relations	1
31	Solution of linear Recurrence Relations	2
32	Solution of in Homogeneous Recurrence Relations	2

33	Tutorial	1
	Total	**40**

Course Designers

1. V.Mohanvmohan@tce.edu
2. S.JeyaBharathisjbmat@tce.edu

Sub Code	Lectures	Tutorial	Practical	Credit

14IS120	3	1	--	4

14IS120 CRYPTOGRAPHY 3:1

Preamble: The course on Cryptography aims at exploring the various cryptographic algorithms deployed in offering confidentiality, integrity, authentication and non repudiation. th Cryptography. The mathematical essentials required for understanding of cryptographic algorithms is also covered in detail.

Program Outcomes addressed

a. Graduates will demonstrate an ability to identify, formulate and solve engineering problems.

c. Graduates will demonstrate an ability to design a system, component or process as per needs and specifications.

e. Graduate will demonstrate skills to use modern engineering tools, softwares and equipment to analyze problems.

Competencies

1. Deploy measures that protect and defend information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation.
2. Determine the strength of a given algorithm used for security service.
3. Analyze threats and vulnerabilities of information systems including databases, networks, applications, internet-based communication, web services, and mobile technologies.

Assessment Pattern

	Bloom's Category	Test 1	Test 2	Test 3	End-semester examination
1	Remember	20	10	10	10
2	Understand	20	20	20	20
3	Apply	40	50	50	50
4	Analyze	20	20	20	20
5	Evaluate	0	0	0	0
6	Create	0	0	0	0

Course Level Learning Objectives

Remember:

1. Define Confidentiality, integrity and Non Repudiation.
2. What is a digital signature?
3. State Discrete Logarithm problem.

4. Enlist the constraints in selecting a key matrix for a Hill Cipher system.
5. What is frequency analysis attack?
6. Define Affine points in an elliptic curve.

Understand:

1. Distinguish between diffusion and confusion.
2. Enumerate the differences between strong and weak collision resistance of hash functions.
3. What do 'unconditionally secure' and 'computationally secure' imply?
4. Draw the Encryption and Decryption scheme of Advanced Encryption Standard.
5. What is the F function? Illustrate by means of a layout diagram the computations involving the 4 S-Box values in blow fish algorithm.
6. Enlist the steps involved in key exchange process of Elliptic Curve Cryptography.

Apply

1. Apply Hill cipher to the message "TCE" with key

   17 7 5 ; 21 18 21 ; 12 2 19
2. Perform encryption and decryption using RSA algorithm for the following:
   a. n=33, M=5 (b) n=55, M=9 (c) n=77, M=8 (d) n=143, M=7 (e) n=527,M=2
3. Given that the round key for the 4th round is e2f467893153f560292f8d7fec2d3712, determine the first 4 bytes of round 5 in AES.
4. Given a message DONKEYSVERSATILE, apply one round of AES and determine the cipher text using the initial key K=MADURAIDESTINATI.
5. The message "DONE" is concatenated with its Frequency Check Sum. This combination is encrypted with the symmetric key K="RUSTE" and transmitted to host B. At the receiving end host B decrypts it using the symmetric key and segregates M||F(M). He then re-computes F(M) and compares it with the received F(M), thereby authenticating the message. Illustrate the above steps. Use ASCII Hex for alphabets.
6. Given E67(2,3), e1=(2,22), d=4, determine e2=d.e1, by first multiplying and then adding twice. Applying ElGamal principle evaluate C1=r.e1 and C2=P+r.e2, Where P is the message (24,26) At the receiving end using C1 and C2, recover the plain text.

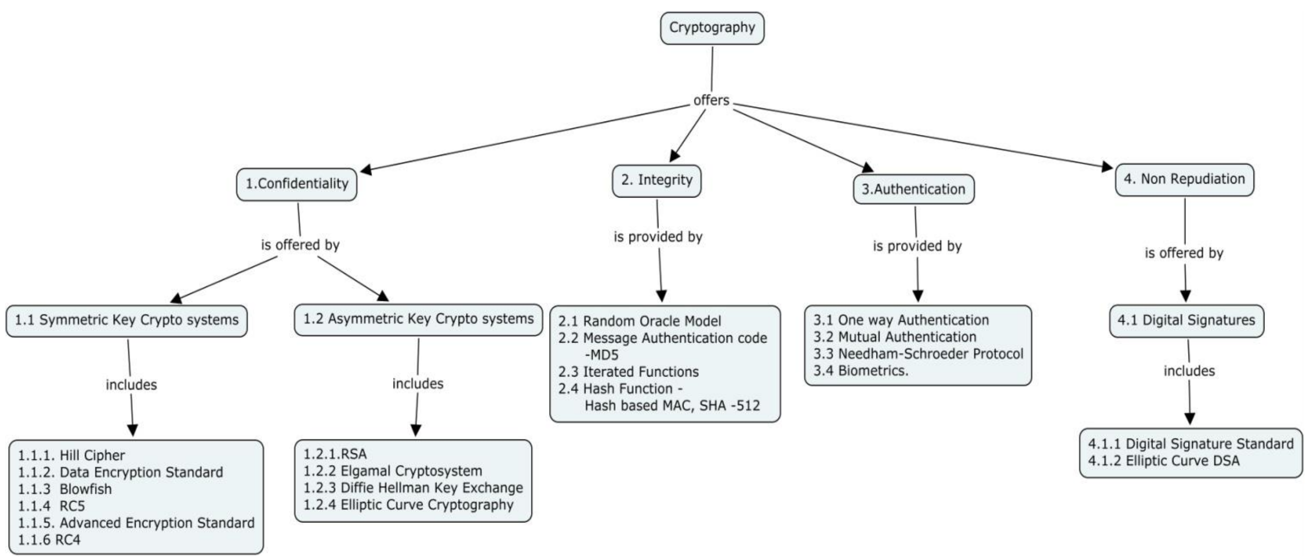
Analyze:

1. Analyze the key management issues involved in symmetric key cryptosystems with respect to public key Cryptosystems.
2. Intercept the message 'FBRTLWUGATEPHBNXSW' which was encoded using a Hill Cipher System with a 3 X 3 key matrix in a 26 letter alphabetic system. The last nine letters are

the sender's signature 'JAMESBOND'. Find the enciphering matrix, deciphering matrix and read the message.

3. Can the following matrix be used as key in Hill cipher? Justify your answer.
   {1,2,3; 4,5,6; 7,8,9}
4. If an adversary is using 2 X 2 enciphering matrix with a 29 letter alphabet, where AZ have the usual numerical equivalents, underscore=26, ?=27, !=28,and the cipher text received is "GFPYJP_X?UYXSTLADPLW" , Crypt analyze the message. (Hint: Last five letters of plain text corresponds to the adversary signature "KARLA").
5. Comment on the strength of mono alphabetic cipher if the language used is Tamil with respect to the number of mappings (Keys).
6. Analyze the threats and vulnerabilities involved in an online examination system.

Concept Map



Syllabus:

Cyber Attacks: Motives, Common Attacks, Defense Strategies and Techniques. **Confidentiality - Symmetric Key Crypto systems**: Modular Arithmetic, Greatest Common Divisor, Multiplicative Inverses, Matrices and Determinants, Inverses, Residue Matrices Hill Cipher, Crypt analysis of Hill Cipher using known plain text –cipher text attack. **Block Ciphers** -Data Encryption standard, Blowfish, RC5, Groups, Rings, Fields, Finite fields of the form GF(p),Finite fields of the form GF(2^n) - Advanced Encryption Standard. **Stream Ciphers** –RC4. **Public key cryptosystems:** Primes, Cardinality of Primes, Eulers totient function, Fermat's and Euler's Theorem, RSA Cryptosystem - Primality testing and Factorization- Square roots modulo 'n', Factoring Algorithms, Attacks and Semantic security on RSA.

Primitive roots, Discrete Logarithm, Diffie Hellman Key Exchange, ElGamal Cryptosystem, Elliptic curve Arithmetic and Elliptic Curve Cryptography, Key Management.

Integrity – Random Oracle Model, Message Authentication Code - MD5, Iterated Functions, Hash Functions – Hash Based MAC, SHA-512.

Authentication: One way Authentication, Mutual Authentication, Needham-Schroeder Protocol, Biometrics.

Non Repudiation: Digital Signature – Digital Signature Standard, Elliptic Curve DSA.

Reference Books

1. Bernard Menezes, Network Security and Cryptography, Cengage Learning 2011.
2. Behrouz A.Foruzan, Cryptography and Network Security, Tata McGraw Hill 2007.
3. William Stallings, Cryptography and Network Security: Principles and Practice", PHI 3rd Edition, 2006.
4. Douglas R. Stinson, "Cryptography Theory and Practice", Third Edition, Chapman & Hall/CRC, 2006

Course Contents and Lectures schedule

S.No	**Topic**	No of Lectures
0	**Cyber Attacks:**	
0.1	Motives, Common Attacks, Defense Strategies and Techniques	1
	Security Services	
1	**Confidentiality – Cryptography**	
1.1	**Symmetric Key Cryptosystems**	1
1.1.1	Modular Arithmetic, Greatest common Divisor, Euclid Algorithm, Multiplicative Inverses	1
1.1.1	Matrices and Determinants, Inverses, Residue Matrices	1
1.1.1	Hill Cipher – Encryption and Decryption	1
1.1.1	Cryptanalysis of Hill Cipher	1
1.1.2	**Block Ciphers -** Data Encryption Standard	2
1.1.3	Blowfish	2
1.1.4	RC5	2
1.1.5	Groups, Rings, Fields	1
1.1.5	Finite fields of the form GF(p), Finite fields of the form GF(2^n)	1

1.1.5	Multiplicative inverse of a polynomial	1
1.1.5	Advanced Encryption Standard	1
1.1.6	**Stream Cipher** – RC4	2
1.2	**Public Key Cryptosystems**	
1.2.1	Primes, Cardinality of Primes, Eulers totient function, Fermat's and Euler's Theorem	2
1.2.1	Primality testing and Factorization	1
1.2.1	RSA	1
1.2.1	Attacks and Semantic Security of RSA	1
1.2.2	Primitive roots, Discrete Logarithm	1
1.2.2	Diffie Hellman Key Exchange	1
1.2.3	Elgamal Cryptosystem	1
1.2.4	Elliptic Curve Arithmetic	2
1.2.4	Elliptic Curve Cryptography	2
1.2.5	Key Management	2
2	**Integrity**	
2.1	Random Oracle Model	1
2.2	Message Authentication Code – MD5	2
2.3	Iterated Functions	1
2.4	Hash Functions – Hash Based MAC, SHA -512	2
3	**Authentication**	
3.1	One way Authentication	1
3.2	Mutual Authentication	2
3.3	Needham-Schroeder Protocol	1
3.4	Biometrics.	2
4	**Non Repudiation**	
4.1	Digital Signatures	1
4.1.1	Digital Signature Standard	1
4.1.2	Elliptic Curve DSA	1
	Total Lectures	**47**

Course Designers:

1. C. Jeyamala jeyamala@tce.edu

2. M.Thangavel mtit@tce.edu

3. A.Divya divyait@tce.edu

Sub Code	Lectures	Tutorial	Practical	Credit
14IS130	**3**	**0**	**--**	**3**

14IS130 Network Security 3:0

Preamble: The course on Network Security focuses on basic concepts of Networks, authentication methods, Protocols, standards, Intrusion Detection and Prevention Mechanisms and Firewalls. It aims to introduce students to the fundamental techniques used in configuring secure networks, and to give them an understanding of common threats and attacks, as well as some practical experience in attacking and defending networked systems. This is **not** a course in cryptography, nor a comprehensive course in systems security. The course will enable the students to understand, develop, and deploy countermeasures to mitigate the risks inherent in the transmission, storage and retrieval of sensitive information and will provide the foundation for doing research in Network security.

Program Outcomes addressed

a. Graduates will demonstrate an ability to identify, formulate and solve engineering problems.

c. Graduates will demonstrate an ability to design a system, component or process as per needs and specifications.

d. An ability to identify, formulate and solve engineering problems.

e. Graduate will demonstrate skills to use modern engineering tools, softwares and equipment to analyze problems.

Competencies

Students will be able to

1. Understand the fundamentals of networks, architecture, Threats and Vulnerabilities.
2. Apply the various Authentication schemes to simulate different applications using APIs.
3. Analyze the different Protocols and standards for various layers and wireless networks.
4. Analyze the various types of Intrusions by detection and prevention mechanisms
5. Apply and analyze different firewalls for different kind of networks.

Assessment Pattern

	Bloom's Category	Test 1	Test 2	Test 3	End-semester examination
1	Remember	20	10	10	10
2	Understand	20	20	20	20
3	Apply	40	50	50	50
4	Analyze	20	20	20	20
5	Evaluate	0	0	0	0
6	Create	0	0	0	0

Course Level Learning Objectives

Remember:

1. Define Network.
2. What is Remote and Wireless Authentication?
3. List out the protocols available in various Network layers.
4. What is Denial of Service attack?
5. Enlist the services and limitations of Firewalls?
6. Define Wi-Fi.

Understand:

1. Distinguish between Attack and Threat.
2. Enumerate the differences between Key distribution and agreement schemes in Authentication.
3. What do 'Network layer' and 'Transport layer' imply?
4. Enlist the steps involved in Intrusion detection process of Worm.
5. Draw the scenario for Packet Inspection Firewall.
6. How Bluetooth provides security in Wireless media.

Apply

1. Suppose that Alice uses the Schnorr Identification Scheme with p=122503, q=1201, t=10, α=357. Now suppose that v=51131, and Olga has learned that
$$\alpha^3 v^{148} \equiv \alpha^{151} v^{1077} \pmod{p}.$$
Show that Olga can compute Alice's Secret exponent α.
2. Consider the following threats to Web security and describe how each is countered by a particular feature of SSL.
    a. Brute-Force Cryptanalytic Attack: An exhaustive search of the key space for a conventional encryption algorithm.

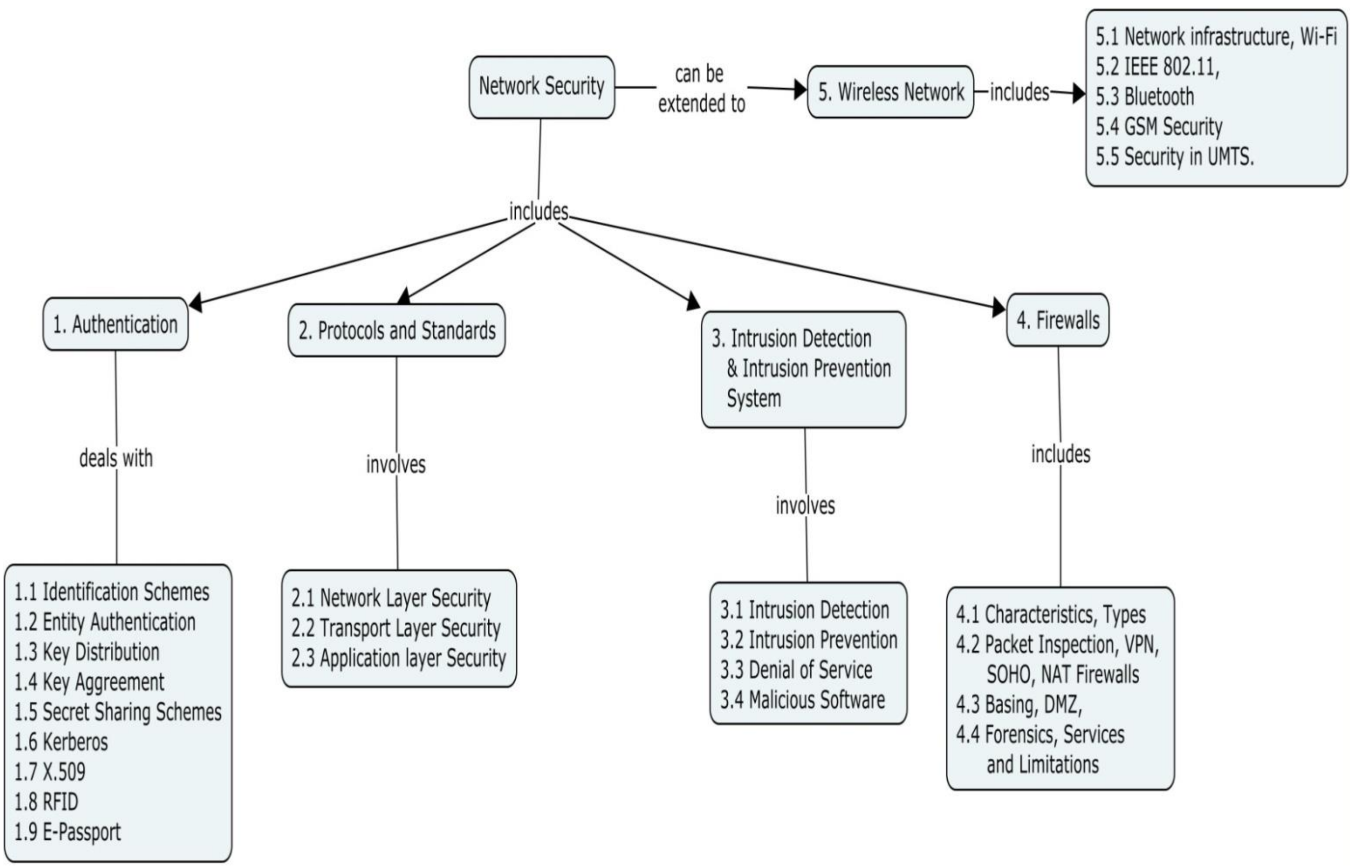
   b. Replay Attack: Earlier SSL handshake messages are replayed.
   c. Man-in-the-Middle Attack: An attacker interposes during key exchange, acting as the client to the server and as the server to the client.
3. In discussing AH processing, it was mentioned that not all of the fields in an IP header are included in MAC calculation.
   a. For each of the fields in the IPv4 header, indicate whether the field is immutable, mutable but predictable, or mutable (zeroed prior to ICV calculation).
   b. Do the same for the IPv6 header.
   c. Do the same for the IPv6 extension headers.
4. Suggest some methods of attacking the PWC worm defense that could be used by worm creators and suggest countermeasures to these methods.
5. In an IPv4 packet, the size of the payload in the first fragment, in octets, is equal to Total Length – (4 ×IHL). If this value is less than the required minimum (8 octets for TCP), then this fragment and the entire packet are rejected. Suggest an alternative method of achieving the same result using only the Fragment Offset field.
6. In IEEE 802.11, open system authentication simply consists of two communications. An authentication is requested by the client, which contains the station ID (typically the MAC address). This is followed by an authentication response from the AP/router containing a success or failure message. An example of when a failure may occur is if the client's MAC address is explicitly excluded in the AP/router configuration.
   a. What are the benefits of this authentication scheme?
   b. What are the security vulnerabilities of this authentication scheme?

Analyze:

1. Consider the following possible identification scheme. Alice possesses a secret key n=pq, where p and q are prime and $p \equiv q \equiv 3 \pmod 4$. The value of n will be stored on Alice's certificate. When Alice wants to identify herself to Bob, say, Bob will present Alice with a random quadratic residue modulo n, say x. Then Alice will compute a square root y of x and give it to Bob. Bob then verifies that $y^2 \equiv x \pmod n$. Explain why this scheme is insecure.
2. Web authorization is central to the security of all Web applications. What is the best way to safeguard all Web applications and at the same time make Web access reliable and fast?
3. The first 16 bits of the message digest in a PGP signature are translated in the clear.
   a. To what extent does this compromise the security of the hash algorithm?

   b. To what extent does it in fact perform its intended function, namely, to help determine if the correct RSA key was used to decrypt the digest
4. For SSH packets, what is the advantage, if any, of not including the MAC in the scope of the packet encryption?
5. An earlier version of WTLS supported a 40-bit XOR MAC and also supported RC4 stream encryption. The XOR MAC works by padding the message with zeros, dividing it into 5-byte blocks and XORing these blocks together. Show that this scheme does not provide message integrity protection.
6. Authentication using certificates, although considered safe, suffers from weaknesses. Discuss these weaknesses using specific examples.

Concept Map



Syllabus

Basics: Computer Network Fundamentals, Network Security, OSI Security Architecture, Security Threats, Vulnerabilities.

Authentication: Elements, types, Methods, Identification Schemes, Entity Authentication, Key Distribution, Key Agreement Schemes, Secret Sharing Schemes, Kerberos, X.509, PKI, Federated Identity Management, RFID, E-Passport.

Protocols and Standards: *Network Layer*: IPSec – Architecture, Authentication Header, Encapsulating Security Payload, Security Policy, IKE, ISAKMP and Virtual private Networks – Tunneling Technologies, Security Considerations. *Transport Layer:* SSL and TLS - Protocols, HTTPS, SSH. *Application Layer:* Email Security –PGP, S/MIME, DKIM. Electronic Payments - SET, Web Services Security.

Intrusion Detection and Prevention – Intrusion Detection: Host, Network, and Hybrid based systems, SIV, LFM, Honeypots, Intrusion Prevention: Host and Network based systems. Denial of Service, DDoS – Prevention, Detection, IP Trace back, Malicious Software, Malware Detection – Worm Detection, Worm Signature extraction, Virus Detection. Case Study: Intrusion Detection Tools.

Firewalls: Characteristics, Types – Packet Inspection, VPN, SOHO, NAT Firewalls, Basing, DMZ, Forensics, Services and Limitations

Wireless Security : Network infrastructure, Wi-Fi, *Standards:* IEEE 802.11, Bluetooth, GSM Security, Security in UMTS.

References:

1. Joseph Migga Kizza, "Computer Network Security", Springer, 2005.
2. Douglas R. Stinson, "Cryptography Theory and Practice", Third Edition, Chapman & Hall/CRC, 2006
3. Network Security and Cryptography, Menezes Bernard, Cengage Learning, New Delhi, 2011
4. William Stallings, "Cryptography and Network Security: Principles and Practices", Fifth Edition, Pearson Education, 2011.
5. Behrouz A.Forouzan, "Cryptography and Network Security", Tata McGarw Hill, 2007.
6. William Stallings, "Network Security Essentials Applications and Standards", Pearson Education, Fourth Edition, 2011
7. William Stallings, Lawrie Brown, "Computer Security: Principles and Practice", First Edition, 2008.
8. "VPN Security", The Government of the Hong Kong Special Administrative Region 2008.

Course Contents and Lecture Schedule

S.No	Topic	No of Lectures
0	**Fundamentals:** Network Security, OSI Security Architecture, Security Threats, Vulnerabilities	1
1.	**Authentication -** Elements, types, Methods	
1.1	Identification Schemes - Federated Identity Management	2

1.2	Entity Authentication	2
1.3	Key Distribution – PKI	2
1.4	Key Agreement Schemes	1
1.5	Secret Sharing Schemes	1
1.6	Kerberos	1
1.7	X.509	1
1.8	RFID	1
1.9	E-Passports	1
2.	**Protocols and Standards**	
2.1	Network Layer Security	1
2.1.1	IPSec	1
2.1.2	VPN	2
2.2	Transport Layer Security	1
2.2.1	SSL	1
2.2.2	TLS	1
2.2.3	HTTPS	1
2.2.4	SSH	1
2.3	Application Layer Security	1
2.3.1	Email Security –PGP, S/MIME, DKIM.	2
2.3.2	Electronic Payments - SET	1
2.3.3	Web Services Security.	2
3.	**Intrusion Detection and Prevention**	
3.1	Intrusion Detection	1
3.1.1	Host, Network, and Hybrid based systems	2
3.1.2	SIV, LFM, Honeypots	1
3.2	Intrusion Prevention	1
3.2.1	Host and Network based systems.	1
3.3	Denial of Service	1
3.3.1	DDoS – Prevention, Detection	1
3.3.2	IP Trace back	1
3.4	Malicious Software	1
3.4.1	Malware Detection – Worm Detection	1
3.4.2	Worm Signature extraction	1
3.4.3	Virus Detection	1

4	**Firewalls**	
4.1	Characteristics, Types	1
4.2	Packet Inspection, VPN, SOHO, NAT Firewalls	1
4.3	Basing, DMZ,	1
4.4	Forensics, Services and Limitations	1
5	**Wireless Security**	
5.1	Network infrastructure, Wi-Fi	1
5.2	IEEE 802.11	1
5.3	Bluetooth	1
5.4	GSM Security	1
5.5	Security in UMTS.	1
	Total Periods	**48**

Course Designers:

1. C. Jeyamala jeyamala@tce.edu

2. M. Thangavel mtit@tce.edu

Sub code	Lectures	Tutorial	Practical	Credit
14IS140	**3**	**1**	**0**	**4**

14IS140 Network Technologies 3:1

Preamble:

This course evokes the architecture and programming APIs of network and also provides in depth knowledge on the functionalities of network and transport layers. It also discusses the recent trends of internetwork field.

Programme Outcomes addressed

Graduates will demonstrate

a) Apply knowledge of mathematics, science, engineering fundamentals and an engineering specialization to the conceptualization of engineering models.

d) Conduct investigations of complex problems including design of experiments, analysis and interpretation of data, and synthesis of information to provide valid conclusions.

l) Recognize the need for, and have the ability to engage in independent and life-long learning.

Competencies

Students will be able to

1. Understand the architecture, functionalities of layers, working principles of various protocols and different topologies.
2. Apply the various networking schemes to simulate different applications using APIs.
3. Apply and analyze different queuing schemes with the given scenario.
4. Analyze the different congestion control and congestion avoidance schemes
5. Comprehend the principles, standards and applications of Software Defined Networks and Network Function Virtualization

Assessment Pattern

	Bloom's Category	Test 1	Test 2	Test 3/End-semester examination
1	Remember	20	20	10
2	Understand	60	50	50
3	Apply	20	20	30
4	Analyze	0	10	10
5	Evaluate	0	0	0
6	Create	0	0	0

Course Level Learning Objectives

Remember:

1. List various layers of OSI model.
2. Define protocol.
3. Describe SDN
4. List the methods of Socket class.
5. Write short notes on virtualization.
6. List the standards of SDN.
7. Draw the architecture of OSI model.

Understand:

1. Explain how the connection establishment and termination happen in TCP.
2. Explain the two different queuing disciplines in transport layer.
3. Discuss the layers functionalities of OSI model.
4. Explain the standards of SDN.
5. Distinguish SDN and NFV.
6. Explain the FIFO queuing technique.
7. Discuss the issues of resource allocation.

Apply:

1. Apply the TCP concept for a chat application using suitable API.
2. Apply the UDP concept to simulate a message passing application using suitable API.
3. Apply the URLConnection class to fetch the data from a particular website.
4. Suppose a router has three input flows and one output. It receives the packets listed in the following table all at about the same time, in the order listed, during a period in which the output port is busy but all queues are otherwise empty. Give the order in which the packets are transmitted. Apply fair queuing.

Packet	Size	Flow
1	100	1
2	100	2
3	150	2
4	200	2
5	50	3
6	190	3

5. Suppose a router has three input flows and one output. It receives the packets listed in the following table all at about the same time, in the order listed, during a period in

which the output port is busy but all queues are otherwise empty. Give the order in which the packets are transmitted. Apply weighted fair queuing, with flow 2 having weight 2, and the other two with weight 1.

Packet	**Size**	**Flow**
1	100	1
2	130	1
3	50	2
4	100	3
5	75	3

6. Give an example of how nonpreemption in the implementation of fair queuing leads to a different packet transmission order from bit-by-bit round-robin service.

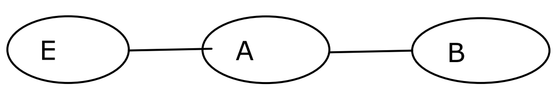
Analyze:

1. Suppose a congestion-control scheme results in a collection of competing flows that achieve the following throughput rates: 100 KBps, 60KBps, 110KBps and 150KBps. Calculate the fairness index for this scheme.
2. Under what circumstances may coarse-grained timeouts still occur in TCP even when the fast retransmit mechanism is being used?
3. During linear increase, TCP computes an increment to the congestion window as

   Increment = MSS x (MSS/CongestionWindow)

Explain why computing this increment each time an ACK arrives may not result in the correct increment. (Hint: A given ACK can acknowledge more or less than one MSS's worth of data).

4.



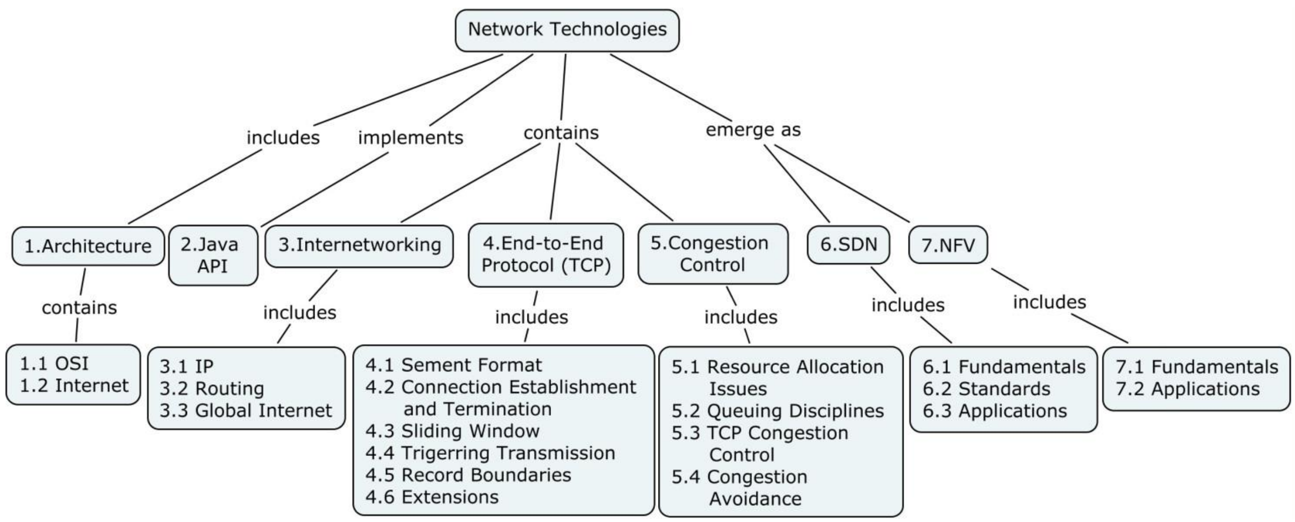
Consider the above simple network, in which A and B exchange distance vector routing information. All links have cost 1.Suppose the A-E link fails

(a) Give a sequence of routing table updates that leads to a routing loop between A & B

(b) Estimate the probability of the scenario in (a), assuming A & B send out routing updates at random times, each at the same average rate.

5. Suppose x and y are two sequence numbers.Write a function to determine whether x comes before y(in the notation of Request for comments 793 “x=<y”) or after y; your solution should work evevn when sequence number wrap around.
6. Analyze why the two-segment-lifetime timeout not necessary on the transition from LAST_ACK to CLOSED when closing a TCP connection.

Concept Map



Syllabus:

Network Architecture: OSI architecture, Internet architecture **Java networking API**, **Internetworking**: IP, Routing, Global Internet **End-to-End Protocols**: TCP – segment format, connection establishment and termination, sliding window, triggering transmission, adaptive retransmission, record boundaries, extensions **Congestion Control:** Resource allocation – issues, queuing disciplines, TCP congestion control, congestion avoidance mechanisms **Software Defined Networks**: Fundamentals, standards, applications **Network Function Virtualization:** Fundamentals and applications.

Reference Books:

1. Larry L.Peterson and Bruce S.Davie, “Computer networks-A system approach”, Elsevier, 2007
2. Herbert Schildt , The complete reference – Java 2, Fifth edition, McGraw-Hill, 2002
3. Ciubotaru, B., Muntean, GM, “Advanced network programming – principles and techniques”, Springer, 2013.
4. Hasan, SF., “Emerging trends in Communication Networks”, Springer, 2014.
5. Thomas D.Nadeau& Ken gray, “Software defined networks”, O’reilly, 2013

Course Contents and Lectures schedule

No	Topic	No. of Lectures
1	**Network Architecture**	
1.2	OSI Architecture	1
1.3	Internet Architecture	1
2	**Java Networking APIs**	3
3	**Internetworking**	
3.1	IP	3
3.2	Routing	3
3.3	Global Internet	3
4	**End-to-End Protocol – TCP**	
4.1	Segment format	2
4.2	Connection establishment and termination	2
4.3	Sliding window	2
4.4	Triggering transmission	2
4.5	Record boundaries	2
4.6	Extensions	2
5	**Congestion Control**	
5.1	Resource allocation – issues	2
5.2	Queuing disciplines	3
5.3	TCP congestion control	3
5.4	Congestion avoidance mechanisms	3
6	**Software Defined Networks (SDN)**	
6.1	Fundamentals	1
6.2	Standards	2
6.3	Applications	2
7	**Network Function Virtualization (NFV)**	
7.1	Fundamentals	1
7.2	Applications	2
	Total	45

Course Designers

1. S.Muthuramalingam smrit@tce.edu

2. P.Karthikeyan karthikit@tce.edu

Sub code	Lectures	Tutorial	Practical	Credit
14IS150	**3**	**1**	**0**	**4**

14IS150 Secure Software Engineering 3:1

Preamble: This course enables students to learn software engineering techniques for building security into software as it is developed (as opposed to reacting to security attacks or about network security or firewall type techniques). Software Security introduces students to the discipline of designing, developing, and testing secure and dependable software-based systems and techniques needed for the practice of effective software security techniques.

Programming Outcomes Addressed

c. Graduates will demonstrate an ability to design a system, component or process as per needs and specifications.

e. Graduates will demonstrate an ability to identify, formulate and solve engineering problems.

k. Graduates will demonstrate skills to use modern engineering tools, software and equipment to analyze problems.

Competencies

Students will be able to

1. Write security requirements (which include privacy requirements).
2. Validate the above requirements and to perform additional verification practices of static analysis and security inspection.
3. Assess the security risk of a system under development
4. Realize the utilization of security metrics.
5. Perform all types of security testing as white box, grey box, and black box/penetration testing.
6. Understand secure coding practices to prevent common vulnerabilities from being injected into software.

Assessment Pattern

	Bloom's Category	Test 1	Test 2	Test 3	End-semester examination
1	Remember	20	10	10	10
2	Understand	20	10	10	10
3	Apply	60	60	40	40
4	Analyze	0	20	40	40
5	Evaluate	0	0	0	0
6	Create	0	0	0	0

Course Level Learning Objectives

Remember

1. Define Software Security
2. List the types of Cryptographic Practices
3. Mention the types of Vulnerabilities in Software Security
4. Define Secure Software Metrics
5. Recall the Properties of Secure Software
6. List the Security Principles and guidelines for Software.

Understand

1. Describe the Threats and Vulnerabilities in Software Security?
2. Briefly explain the steps in Secure SDLC.
3. Differentiate SDLC and Secure SDLC.
4. Explain the Cryptographic Practices for Secure Programming and tell about its merits over other secure coding practices.
5. Illustrate the need for Secure Programming with Data Validation.
6. Explain the Risk Analysis Process in Secure Software Design

Apply

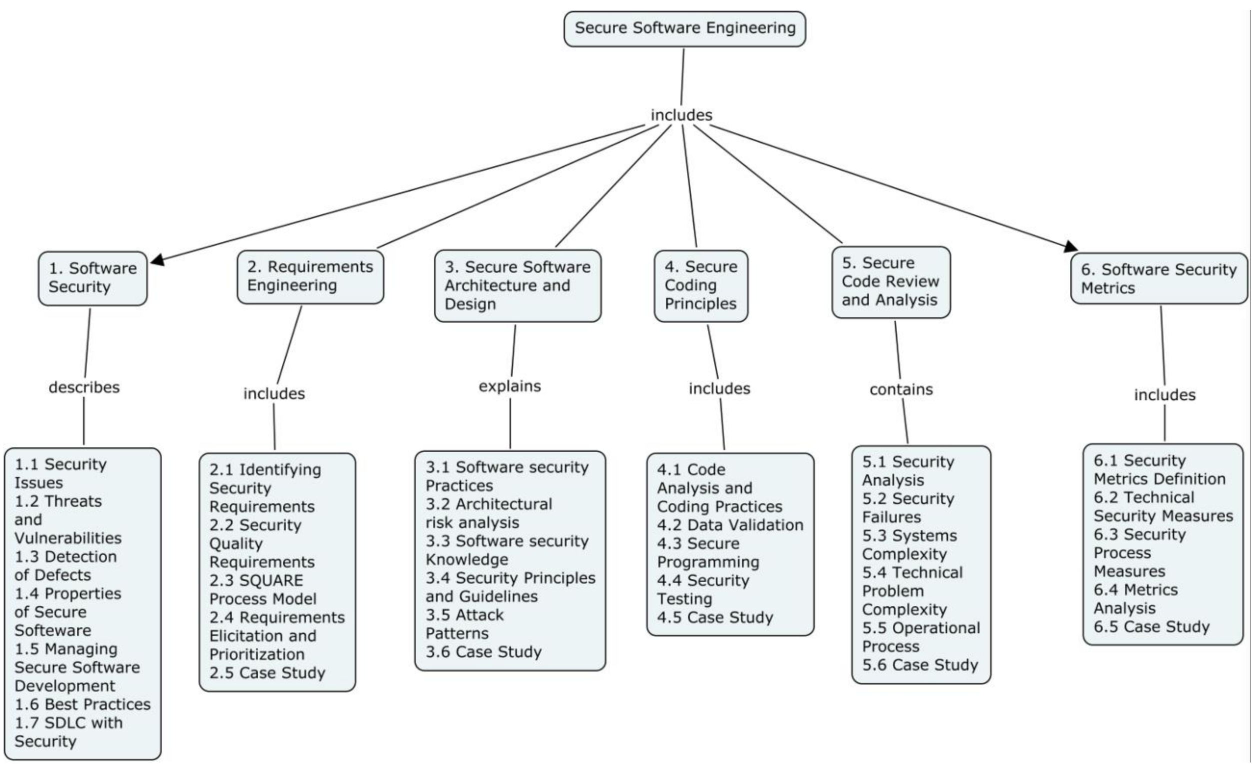
1. Apply Security testing that validate that the internal program logic and produce valid outputs for ATM Application . All decision branches and internal code flow should be validated.
2. Design a new secure interface for a college Mark entry system. Academic and Administrative staff use this system heavily during examination time. What Cryptographic practices will you adapt for the design.

3. Identify the Attack Patterns and necessary security principles and guidelines for Workshop registration.
4. Validate the requirements and perform additional verification practices of static analysis and security inspection for Secure Banking application.

Analyze

1. Boundary use cases are not described during Secure requirements elicitation or analysis. Justify your answer.
2. Consider an application that must select dynamically an encryption algorithm based on security requirements and computing time constraints. Analyze the design pattern that can be selected.
3. Illustrate with the scenarios how Data Validation is beneficial to developers in Software Design.
4. Identify, analyze, prioritize and plan for the top five risks associated with the Secure design of MyTrip subsystem.

Concept Map



Syllabus:

Software Security – Secure Software Engineering Issues, Threats and Vulnerabilities , Secure SDLC Properties **Requirements Engineering** – Secure Requirements Elicitation, Managing Quality Requirements, SQUARE PROCESS MODEL, Case Study **Secure Software**

Architecture and Design – Architectural Risk Analysis, Security Principles , Attack Patterns , Case Study **Secure Coding** – Principles, Data Validation, Cryptographic Practices, Case Study **Code Review and Analysis** – Security Analysis , Security Failures, System Complexity , Operational Process , Case Study **Security Metrics** – Software Security and Process measures , Metric Analysis, Case Study

References

1. Software Security Engineering: A Guide for Project Managers, by Julia H. Allen, Sean Barnum, Robert J. Ellison, Gary McGraw, Nancy R. Mead, Addison-Wesley , 1st edition, 2008.
2. Security Metrics: Replacing Fear, Uncertainty, and Doubt , by Andrew Jaquith, Addison-Wesley , 1st edition , 2007.
3. Ross J Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, 2ndEdition, Wiley, 2008.
4. Integrating Security and Software Engineering: Advances and Future Vision, by Haralambos Mouratidis, Paolo Giorgini, IGI Global, 2006.
5. Software Security: Building Security In , by Gary McGraw , Addison-Wesley, 2006
6. The Art of Software Security Assessment: Identifying and Preventing Software Vulnerabilities, by Mark Dowd, John McDonald, Justin Schuh, Addison-Wesley, 1st edition, 2006
7. Building Secure Software: How to Avoid Security Problems the Right Way by John Viega,Gary McGraw, Addison-Wesley, 2001
8. Writing Secure Code, by M. Howard, D. LeBlanc, Microsoft Press, 2nd Edition, 2003.
9. Exploiting Software: How to break code, by G. Hoglund, G. McGraw,Addison Wesley, 2004.

Course Contents and Lecture Schedule

S.No	Topic	No.of Lectures
1	**Software Security**	
1.1	Security issues	1
1.2	Threats and Vulnerabilities	1
1.3	Detection of Defects	1
1.4	Properties of Secure Software	1
1.5	Managing Secure Software Development	1

1.6	Software Security Best practices	1
1.7	SDLC with Security	1
2	**Requirements Engineering**	
2.1	Identifying Security Requirements	1
2.2	Security Quality Requirements	1
2.3	SQUARE Process Model	1
2.4	Requirement Elicitation and Prioritization	1
2.5	Case Study	1
3	**Secure Software Architecture and Design**	
3.1	Software Security Practices	2
3.2	Architectural Risk Analysis	1
3.3	Software Security Knowledge	1
3.4	Security Principles and Security Guidelines	2
3.5	Attack Patterns	1
3.6	Case Study	1
4	**Secure Coding Principles**	
4.1	Code analysis and Coding practices	2
4.2	Data Validation	1
4.2.1	Input Validation and Output encoding	1
4.2.2	Session and Authentication, Password Management	1
4.2.3	Access Control, Communication and Database Security	1
4.2.4	System Configuration, Data Protection and File Management	2
4.3	Secure Programming : Cryptographic Practices	2
4.4	Security Testing	3
4.5	Case Study	1
5	**Secure Code Review and Analysis**	
5.1	Security Analysis	1
5.2	Security Failures	1
5.3	Systems complexity	1
5.4	Technical Problem Complexity	2
5.5	Operational Process	1
5.6	Case Study	1
6	**Software Security Metrics**	
6.1	Security Metrics Definition	1

6.2	Technical Security Measures	1
6.3	Security Process Measures	1
6.4	Metrics Analysis	1
6.5	Case Study	1
	Total Lectures	**46**

Course Designer:

1. M.Abiramiabiramiam@tce.edu
2. M.Ayswharya Devi ayswharyadevimadhavan@tce.edu

Sub Code	Lectures	Tutorial	Practical	Credits
14IS160	3	1	-	4

14IS160 Data Base Security **3:1**

Preamble: This course aims at facilitating the student to understand the various functionalities of DBMS, to perform many operations related to creation, usage and maintenance of databases for real-world applications. Also it concerns the use of broad range of information security controls to protect databases against compromises of confidentiality, integrity and availability using various categories of controls, procedural and administrative audits.

Programming Outcomes Addressed

d. Graduates will demonstrate an ability to design a system, component or process as per needs and specifications.
e. Graduates will demonstrate an ability to identify, formulate and solve engineering problems.
l. Graduates will demonstrate skills to use modern engineering tools, software and equipment to analyze problems.

Competencies

At the end of the course the student will be able to

1. Understand the database design and implementation
2. Describe the basic relational model, its integrity constraints, update operations and the operations of the relational algebra.
3. Use the formalisms, theory and algorithms developed for relational database design by normalization.
4. Explain authentication, authorization and Identify, use database password best practices
5. know SQL injection and identify how injections are executed
6. Describe methods for automatic traversing of source code to locate injection vulnerability
7. Define SQL injection exploitation and identify defensive strategies against the exploits
8. Illustrate the database trust management and auditing services.

Assessment Pattern

	Bloom's Category	Test 1	Test 2	Test 3	End-semester Examination
1.	Remember	20	20	20	20
2.	Understand	30	20	20	30
3.	Apply	50	30	30	30
4.	Analyze	0	30	30	20
5.	Evaluate	0	0	0	0
6.	Create	0	0	0	0

Course Level Learning Objectives

Remember

1. Define the data model in data bases?
2. List the different constraints exist in SQL?
3. Recall any four notations in ER model?
4. Enlist the merits of DBMS
5. Recognize the conversion functions.
6. Write the authentication options supported by DB2 UDB 8.2.

Understand

1. Describe the three schema architecture of DBMS.
2. Explain the join dependency and its types with an example.
3. Illustrate the role of different components in Data Base system environment.
4. Discuss the categories classified for data base management systems.
5. Review where and how the database users and passwords are maintained.

Apply

1. Compare and contrast the DBMS with respect to File System.
2. Use SQL Statements to create STUDENT, FACULTY, COURSE, ADMINISTRATION, DEPARTMENT tables for COLLEGE database and apply all the constraints and integrity rules wherever appropriate.
3. Write the SQL statements to create the BOOKS, COPIES _ISSUED _TO _BORROWER, BORROWER and LIBRARY _STAFF of LIBRARY database. Remove a book named "data structures" and the author name is "shani" from the library .Get the list of books by a particular author or in a particular subject area .Display the concatenated format of

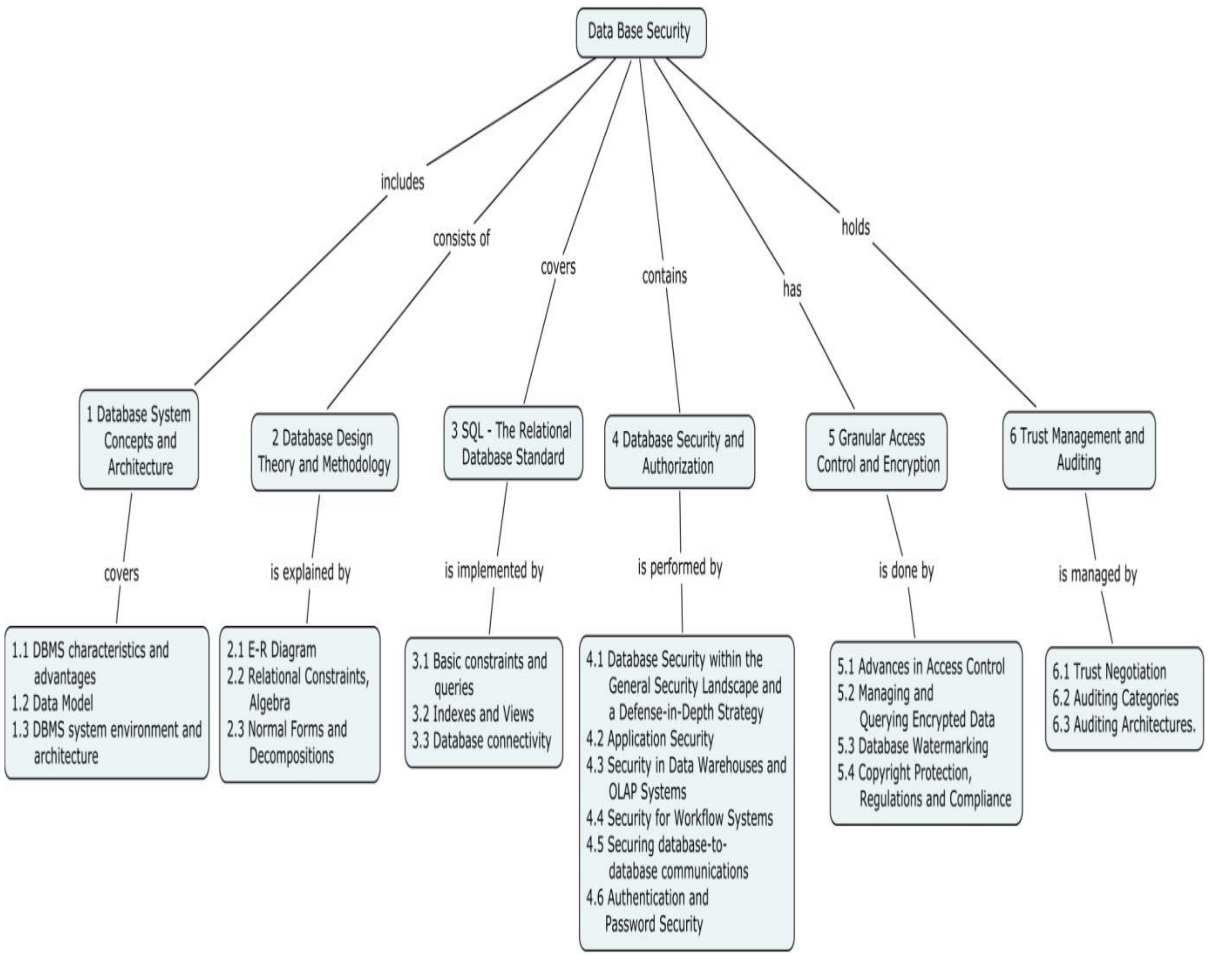
"staff names "*is working as* "their designation". Rename a column name of PUBLISHER in books table as "BOOK PUBLISHER". Give 15% raise in the salary to the staff ID=111 .Get the list of books which is having more than 4 copies.

4. For the above table used in question 3 List the faculty advisor of student from student and faculty tables. Display the book names start with "d". Get the list of library staff members who is having highest salary and who is having lowest salary. Write the output for this query "SELECT UPPER (STAFF NAME), (SYSDATE-HIREDATE) DAYS from LIBRARY _STAFF ORDER BY DAYS. Add a column as "return date" which will be automatically calculated from the issue date and display the return date from 14 days after the issue date.
5. Draw an ER model for organization data base for the relationships Employee-Department and Employee-Projects.
6. You have been hired as the security consultant for TJRiggings. As your first task, you have been asked to complete a security audit of their Web applications. Answer the following questions:
   i. Identify the first step that you would take to test the sites for SQL injection vulnerability? And apply the concept of inferential testing?
   ii. Use your strategy for identifying dangerous source code now and far into the future?
   iii. Produce your suggestions for offering TJRiggings in reference to their Web clients?

Analyze

1. Characterize the Database Watermarking for Copyright Protection.
2. Classify the various levels of security for banking application.
3. Dramatize that how the anomalies are handled and decompose the table based on dependencies.
4. Select the mechanism used to secure the replicated data in communication.
5. Examine technique for audit trail analysis.
6. Identify the use of visualization for security policies.

Concept Map



Syllabus

Database System Concepts and Architecture – DBMS characteristics and advantages - Data Model –DBMS system environment and architecture- **Database Design Theory and Methodology** – E-R Diagram - Relational Constraints, Algebra- Normal Forms and Decompositions - **SQL - The Relational Database Standard** – Basic constraints and queries - Indexes and Views - Database connectivity - **Database Security and Authorization** - Database Security within the General Security Landscape and a Defense-in-Depth Strategy - Application Security - Security in Data Warehouses and OLAP Systems - Security for Workflow Systems - Securing database-to-database communications - Authentication and Password Security -**Granular Access Control and Encryption** - Advances in Access Control - Managing and Querying Encrypted Data -Database

Watermarking - Copyright Protection, Regulations and Compliance - **Trust Management and Auditing** - Trust Negotiation - Auditing Categories - Auditing Architectures.

REFERENCES:

1. Elamsri, Navathe, Somayajulu and Gupta, Database Concepts, Pearson Edu, 2006.
2. Michael Gertz, Sushil Jajodia, Handbook of Database Security: Applications and Trends, Springer,2008.
3. Nilesh Shah, "Database Systems using Oracle", 2nd edition, Prentice Hall of India Pvt Ltd, 2007.
4. Ron Ben Natan, "Implementing Database Security and Auditing", Elsevier, 2005.
5. Alfred Basta, Melissa Zgola, Dana Bullaboy, Thomas L.Whitlock Sr.," Database Security", Cencage Learning, 2012.
6. Bhavani Thuraisingham, "Database and Applications security – Integrating Information security and Data Management", Taylor & Francis Group, 2005.

Course contents and Lectures Schedule:

S.No.	Topic	No. of Lectures
1	**Database System Concepts and Architecture**	
1.1	DBMS characteristics and advantages	1
1.2	Data Model	1
1.3	DBMS system environment and architecture	2
2	**Database Design Theory and Methodology**	
2.1	E-R Diagram	2
2.2	Relational Constraints, Algebra	2
2.3	Normal Forms and Decompositions	2
3	**SQL - The Relational Database Standard**	
3.1	Basic constraints and queries	5
3.2	Indexes and Views	1
3.3	Database connectivity	1
4	**Database Security and Authorization**	2
4.1	Database Security within the General Security Landscape and a Defense-in-Depth Strategy	3
4.2	Application Security	5

S.No.	Topic	No. of Lectures
4.3	Security in Data Warehouses and OLAP Systems	2
4.4	Security for Workflow Systems	1
4.5	Securing database-to-database communications	2
4.6	Authentication and Password Security	3
5	**Granular Access Control and Encryption**	**2**
5.1	Advances in Access Control	2
5.2	Managing and Querying Encrypted Data	1
5.3	Database Watermarking	1
5.4	Copyright Protection, Regulations and Compliance	1
6	**Trust Management and Auditing**	**1**
6.1	Trust Negotiation	2
6.2	Auditing Categories	2
6.3	Auditing Architectures	3
	Total	**50**

Course Designers:

M.NirmalaDevi mnit@tce.edu

E.Ramanujam erit@tce.edu

Sub Code	Lectures	Tutorial	Practical	Credits
14IS170	-	-	3	1

14IS170 – Cryptography and Network Security Lab

Preamble :

The laboratory course on Cryptography and Network security will enable the students to gain hands on experience in implementation of cryptographic algorithms and tools used in security analysis and forensics.

List of Experiments

Tools Required : Open SSL, Wire Shark, DVWA, NMAp, Nessus, OSSEC, Pflogsum

1. Implementation of Known Plain text attack in Hill Cipher
2. Implementation of Data Encryption Standard
3. Implementation of Advanced Encryption Standard
4. Implementation of RSA
5. Implementation of Least Significant Bit method in Image Steganography
6. Security Analysis of Cryptographic algorithms using OPEN SSL
7. Analysis of Secure Socket Layer and IPSec protocol using wireshark
8. Simulation of SQL injection using DVWA
9. Simulation of Cross site Scripting using DVWA
10. Port Scanning using Nmap and Buffer overflow
11. Forensic Analysis using OSSEC
12. Email log Reports using Pflogsum

Course Designers :

1. C.Jeyamala jeyamala@tce.edu
2. M.Thangavel mtit@tce.edu

CURRICULUM AND DETAILED SYLLABI

FOR

M.E DEGREE (COMPUTER SCIENCE AND INFORMATION SECURITY) PROGRAMME

SECOND SEMESTER

FOR THE STUDENTS ADMITTED IN THE

ACADEMIC YEAR 2014-15 ONWARDS

THIAGARAJAR COLLEGE OF ENGINEERING
(A Government Aided ISO 9001:2008 certified Autonomous Institution affiliated to Anna University)
MADURAI – 625 015, TAMILNADU

Phone: 0452 – 2482240, 41
Fax: 0452 2483427
Web: www.tce.edu

THIAGARAJAR COLLEGE OF ENGINEERING: MADURAI – 625 015
M.E (Computer Science and Information Security) Degree Programme

COURSES OF STUDY
(For the candidates admitted from 2014-15 onwards)

SECOND SEMESTER

Course Code	Name of the Course	Category	No. of Hours / Week			credits
			L	T	P	
THEORY						
14IS210	System Security	PC	3	1	-	4
14IS220	Data Analytics	PC	3	-	-	3
14IS230	Wireless Security	PC	3	1	-	4
14ISPX0	Elective- I	PE	3	1	-	4
14ISPX0	Elective- II	PE	3	1	-	4
14ISPX0	Elective- II	PE	3	1	-	4
PRACTICAL						
14IS270	Data Analytics Lab	PC	-	-	2	2
Total			**18**	**5**	**2**	**25**

BS : Basic Science
HSS : Humanities and Social Science
ES : Engineering Science
PC : Program Core
PE : Program Elective
GE : General Elective

L : Lecture
T : Tutorial
P : Practical

Note:

1 Hour Lecture is equivalent to 1 credit

2 Hours Tutorial is equivalent to 1 credit

2 Hours Practical is equivalent to 1 credit

THIAGARAJAR COLLEGE OF ENGINEERING: MADURAI – 625 015

M.E (Computer Science and Information Security) Degree Programme

SCHEME OF EXAMINATIONS
(For the candidates admitted from 2014-15onwards)

SECOND SEMESTER

S.No.	Course Code	Name of the Course	Duration of Terminal Exam. in Hrs.	Marks			Minimum Marks for Pass	
				Continuous Assessment *	Terminal Exam **	Max. Marks	Terminal Exam	Total
THEORY								
1	14IS210	System Security	3	50	50	100	25	50
2	14IS220	Data Analytics	3	50	50	100	25	50
3	14IS230	Wireless Security	3	50	50	100	25	50
4	14ISPX0	Elective- I	3	50	50	100	25	50
5	14ISPX0	Elective- II	3	50	50	100	25	50
6	14ISPX0	Elective- III	3	50	50	100	25	50
PRACTICAL								
1	14IS270	Data Analytics Lab	3	50	50	100	25	50

* CA evaluation pattern will differ from course to course and for different tests. This will have to be declared in advance to students. The department will put a process in place to ensure that the actual test paper follow the declared pattern.

** Terminal Examination will be conducted for maximum marks of 100 and subsequently be reduced to 50 marks for the award of terminal examination marks

		Category	L	T	P	Credit
14IS210	**SYSTEM SECURITY**	PC	3	1	0	4

Preamble

This course provides a deep and comprehensive study of the security principles and practices of computer systems. Topics include common attacking techniques, non-cryptographic tools, authentication and access control and software security.

Prerequisite

- 14IS130: Network Security

Course Outcomes

On the successful completion of the course, students will be able to

Course Outcomes		**Bloom's Level**
CO1:	State the requirements and mechanisms for identification and authentication of the system.	Understand
CO2:	Explain concepts related to various non-cryptographic, malicious software and vulnerabilities.	Understand
CO3:	Appraise various access control policies on various Operating systems.	Apply
CO4:	Illustrate appropriate mechanisms for protecting information systems ranging from operating systems, to database management systems, and to real time applications.	Analyze

Mapping with Programme Outcomes

COs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11
CO1	**L**										
CO2	**L**										
CO3	**M**	**M**			**L**						
CO4	**S**	**S**	**M**		**M**	**M**		**M**	**M**	**L**	

S- Strong; M-Medium; L-Low

Assessment Pattern

Bloom's Category	**Continuous Assessment Tests**			**Terminal Examination**
	1	**2**	**3**	
Remember	30	10	0	20
Understand	30	20	20	20
Apply	40	40	40	40
Analyse	0	30	40	20
Evaluate	0	0	0	0
Create	0	0	0	0

Course Level Assessment Questions

Course Outcome 1 (CO1):

1. Explain the requirement of sequence numbers in authentication.
2. Write in detail about the various ways to implement biometrics.
3. Explain how authentication service can be implemented? List the protocols used for authentication.

Course Outcome 2 (CO2):

1. What is the classification of attacks? Compare and contrast both the types.
2. What are the variations of Dos attack? Explain them.
3. Explain about DDoS attacks. How zombies can be used to create DDos?
4. Explain how the vulnerability may be exploited leading to an attack in the design of TCP and UCP Protocols.

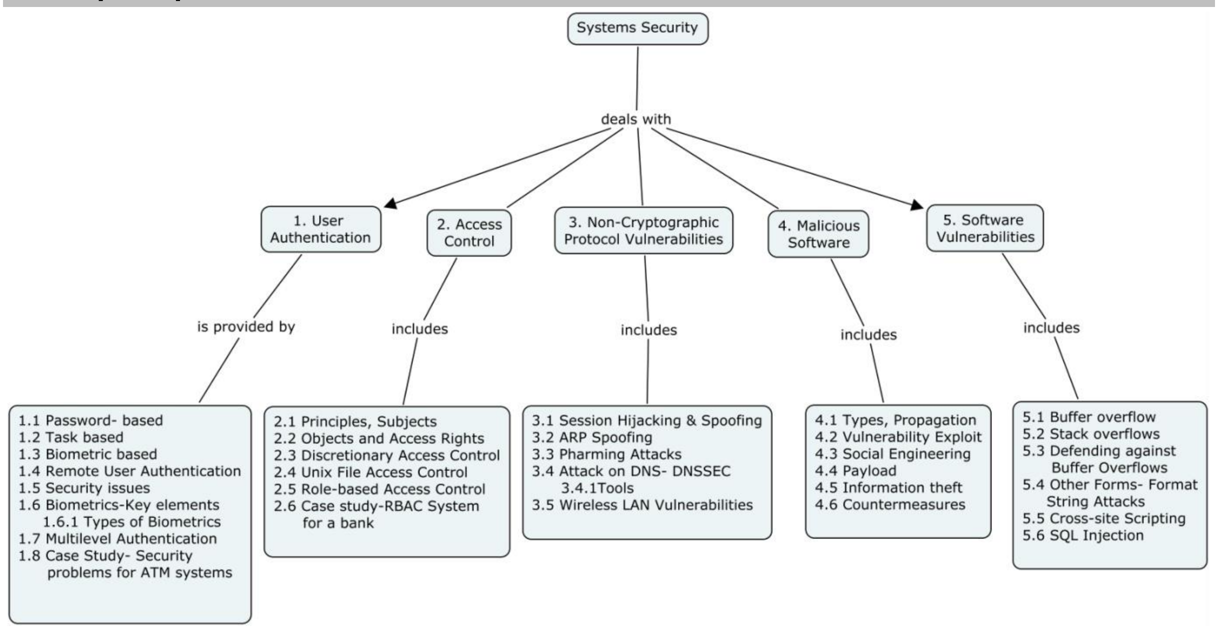
Course Outcome 3 (CO3):

1. State and briefly explain two or three of the most compelling positive aspects/ features and two or three drawbacks and limitations of access control in each of unix, windows and SELinux.
2. What are some reasonable filtering rules for a kernel-based packet screen?
3. Name some reasonable filtering rules for a Cisco?
4. Distinguish between the terms rights and privileges, role and group.

Course Outcome 4 (CO4):

1. You are assigned a job of system administrator of a company. Explain how will you try to secure your own network from the following agents that pose a threat to the security:
    1) Worms
    2) Hackers
    3) Cookies
    4) Employees
2. How might I increase the security and scalability of my DMZ (demilitarized zone)?
3. Design a mobile payment scheme that does not require the cell phone owner to download or install any special payment related code. Can such a scheme be secure? Explain why or why not.

Concept Map



Syllabus

User Authentication: Password- based, Task based, Biometric based, Remote User Authentication, Security issues, Biometrics-Key elements- Types of Biometrics- Finger print- Hand Geometry- Face and Voice Recognition- Eye Biometrics- Iris and Retina Scanning- Signature Recognition- Multilevel Authentication- Case Study- Security problems for ATM systems.

Access Control: Principles, Subjects, Objects and Access Rights, Discretionary Access Control, Example- Unix File Access Control, Role-based Access Control, Case study-RBAC System for a bank.

Non-Cryptographic Protocol Vulnerabilities: Session Hijacking and Spoofing- ARP Spoofing- Pharming Attacks- Attack on DNS- DNSSEC- Tools-Wireless LAN Vulnerabilities.

Malicious Software: Types, Propagation- Infected Content, Viruses, Vulnerability Exploit- Worms, Social Engineering-Spam, E-mail, Trojans, Payload-system corruption, Attack agent, Zombie, Bots, Information theft- Key loggers, Phishing, Spyware, Steal thing, Backdoors, Root kits, Countermeasures- Mobile Malware.

Software Vulnerabilities: Buffer overflow- Stack overflows-Defending against Buffer Overflows-Other Forms- Format String Attacks- Cross-site Scripting-XSS vulnerabilities- Overcoming XSS-SQL Injection.

Textbook

1. W. Stallings, "Computer Security: Principles and Practice," 3rd Edition, Prentice Hall, , 2013.
2. Bernard Menezes, "Network Security and Cryptography", 1/e, Cengage Learning India, 2010.

Reference Books

1. M. Stamp, "Information Security: Principles and Practice," 2st Edition, Wiley, ISBN: 0470626399, 2011.
2. M. E. Whitman and H. J. Mattord, "Principles of Information Security," 4st Edition, Course Technology, ISBN: 1111138214, 2011.
3. M. Bishop, "Computer Security: Art and Science," Addison Wesley, ISBN: 0-201-44099-7, 2002.
4. G. McGraw, "Software Security: Building Security In," Addison Wesley, ISBN: 0321356705, 2006.
5. John Woodword, Nicholas, "Biometrics: The Ultimate Reference", John Wiley & Sons, 2003.

Course Contents and Lecture Schedule

Module .No	Topic	No. of Lectures
1.	**User Authentication**	
1.1	Password- based	1
1.2	Task based	1
1.3	Biometric based	1
1.4	Remote User Authentication	1
1.5	Security issues	2
1.6	Biometrics-Key elements	1

Module .No	Topic	No. of Lectures
1.6.1	Types of Biometrics- Finger print- Hand Geometry- Face and Voice Recognition-Eye Biometrics- Iris and Retina Scanning- IRIS biometric system, Signature Recognition	3
1.7	Multilevel Authentication	2
1.8	Case Study- Security problems for ATM systems	1
2	**Access Control**	
2.1	Principles, Subjects	2
2.2	Objects and Access Rights	1
2.3	Discretionary Access Control	1
2.4	Unix File Access Control	2
2.5	Role-based Access Control	2
2.6	Case study-RBAC System for a bank	1
3	**Non-Cryptographic Protocol Vulnerabilities**	
3.1	Session Hijacking and Spoofing	2
3.2	ARP Spoofing	1
3.3	Pharming Attacks	1
3.4	Attack on DNS- DNSSEC	2
3.4.1	Tools	1
3.5	Wireless LAN Vulnerabilities	1
4	**Malicious Software**	
4.1	Types, Propagation- Infected Content, Viruses	2
4.2	Vulnerability Exploit- Worms	1
4.3	Social Engineering-Spam, E-mail, Trojans	2
4.4	Payload-system corruption, Attack agent, Zombie, Bots	1
4.5	Information theft-Key loggers, Phishing, Spyware, Steal thing,	2
4.6	Countermeasures- Mobile Malware	2
5	**Software Vulnerabilities**	
5.1	Buffer overflow	1
5.2	Stack overflows	1
5.3	Defending against Buffer Overflows	1
5.4	Other Forms- Format String Attacks	1
5.5	Cross-site Scripting-XSS vulnerabilities- Overcoming XSS	2
5.6	SQL Injection	2
	Total Lectures	**48**

Course Designers:

1. E. Ramanujam erit@tce.edu
2. R. Parkavi rpit@tce.edu
3. S.Sujitha sujithait@tce.edu

			Category	L	T	P	Credit
14IS220	**DATA ANALYTICS**		PC	3	0	0	3

Preamble

The course on Data Analytics aims to emphasize the need for and provide an in depth coverage of various analytics techniques. This course aims at facilitating the student to understand the various functionalities of Data Analytics and perform many operations related to creating, using and maintaining databases for Real-world applications and emerging technologies in Data Analytics.

Prerequisite

- Nil

Course Outcomes

On the successful completion of the course, students will be able to

Course Outcomes		**Blooms Level**
CO1:	Express the data analytics process model.	Understand
CO2:	Solve different data pre-processing techniques.	Apply
CO3:	Demonstrate different predictive models.	Analyze
CO4:	Examine Survival Analysis model and learn through Social Network Analytics.	Analyze

Mapping with Programme Outcomes

COs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11
CO1.	L	L							L		
CO2.	L	L			M				L	L	
CO3.	M	L	L		S			M	M	M	
CO4.	S	M	M	L	S	L		L	M	M	

S- Strong; M-Medium; L-Low

Assessment Pattern

Bloom's Category	Continuous 1	Continuous 2	Continuous 3	Terminal Examination
Remember	30	20	0	0
Understand	30	30	30	30
Apply	20	30	40	40
Analyse	20	20	30	30
Evaluate	0	0	0	0
Create	0	0	0	0

Course Level Assessment Questions

Course Outcome 1 (CO1):

1. Identify the requirements of an analytics process model.
2. Describe the Analytics process model?
3. Mention some of the data analytics applications.

Course Outcome 2 (CO2):

1. Compute the technique of sampling and pre-processing for the data set of a bank application. Identify the fields and labels over the dataset and perform all the steps over pre-processing technique.
2. Differentiate among sampling and data pre-processing.
3. Clearly explain the process of filling in the missing values in data pre-processing.

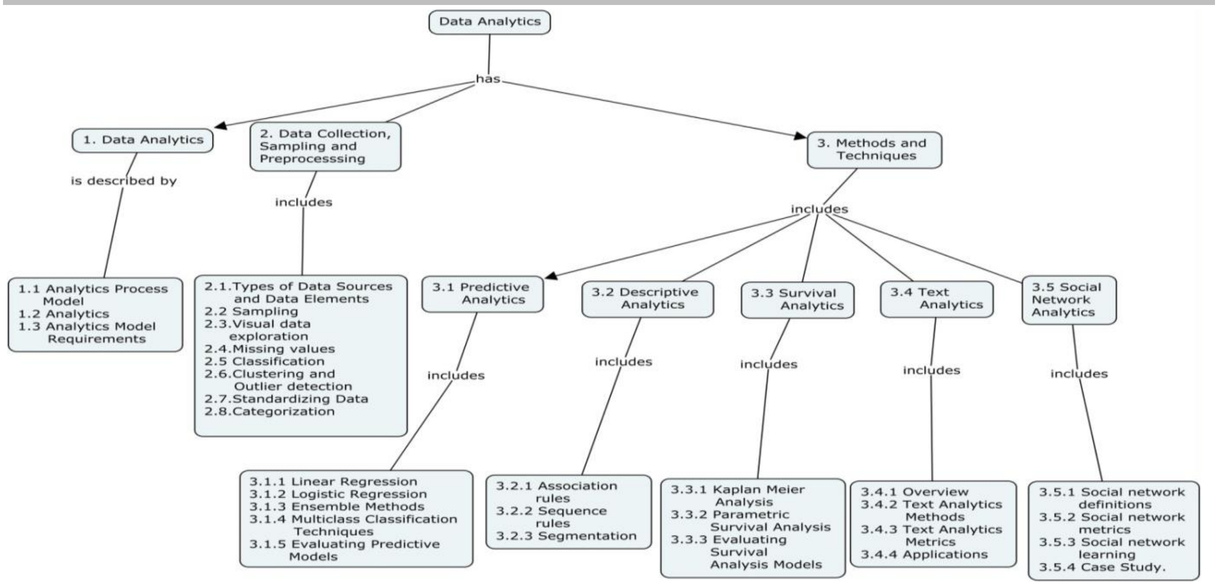
Course Outcome 3 (CO3):

1. Prepare a predictive model for resource utilization by a computer system which has maximum size of RAM 512 MB, and 120 GB hard disk, which runs 6 processes at a given time with the time allotted for each of the process is about 2 milliseconds.
2. Point out the need for using a multiclass classification model in a system. Clearly provide the reasons over binary classification system with necessary illustrations
3. Depict a predictive model using multiclass classification techniques for any real-time application.

Course Outcome 4 (CO4):

1. Interrogate the metrics and the methods in social network analytics for a bank ATM system with the standard for classifying the system into different sets of sub parts and justify with your proposed analytical model.
2. Consider an application of hospital management system which contains records of large set of patients in various diseases such as diabetes, heart disease, cancer. Apply the concept of ensemble methods to overcome the difficulties in maintaining the records in various departments in the hospital and also justify with the method that you have chosen for evaluation with the classification of the datasets across different disciplines.
3. Differentiate Kaplan Meier Analysis and parametric survival analysis.
   Use ego nets and bigraphs for content management system.

Concept Map



Syllabus

Data Analytics: Analytics Process Model – Analytics – Analytical Model Requirements

Data Collection, Sampling and Preprocessing: Types of Data Sources and Data Elements– Sampling – Visual Data Exploration – Missing Values –Classification-Clustering and Outlier detection – Standardizing data – Categorization

Predictive Analytics: Linear Regression – Logistic Regression – Ensemble Methods – Multiclass Classification Techniques – Evaluating Predictive Models

Descriptive Analytics: Association rules – sequence rules –segmentation

Survival Analytics: Kaplan Meier Analysis –Parametric Survival Analysis – Evaluating Survival Analysis Models

Text Analytics: Overview – Text Analytics Methods – Text Analytics Metrics – Applications

Social Network Analytics: Social network definitions – Social network metrics –Social network learning – Case Study on Real-Time Applications.

Reference Books

1. Bart Baesens, “Analytics in a Big Data World”, The Essential Guide to Data Science and its Applications, Wiley, First edition,2014.
2. Thomas H. Davenport, Jeanne G. Harris, “Competing on Analytics: The New Science of Winning”, Harvard Business Review Press ,First edition,2007
3. Paul C. Zikopoulos, Chris Eaton, “Understanding Big Data”, McGraw-Hill, 2012 (eBook from IBM)

Websites

1. http://www.bigdatauniversity.com

Course Contents and Lecture Schedule

Module No.	Topic	No. of Lectures
1.	**Data Analytics**	
1.1	Analytics Process Model	2
1.2	Analytics	1
1.3	Analytical Model Requirements	1
2	**Data Collection, Sampling and Pre-processing**	
2.1	Types of Data Sources and Data Elements	1
2.2	Sampling	1
2.3	Visual Data Exploration	1
2.4	Missing Values	1
2.5	Classification	1
2.6	Clustering and Outlier Detection	1
2.7	Standardizing data	1
2.8	Categorization	1
3	**Methods and Techniques**	
3.1	**Predictive Analytics**	
3.1.1	Linear Regression	1
3.1.2	Logistic Regression	1

Module	Topic	No. of Lectures
3.1.3	Ensemble Methods	1
3.1.4	Multiclass Classification Techniques	2
3.1.5	Evaluating Predictive Models	2
3.2	**Descriptive Analytics**	
3.2.1	Association rules	1
3.2.2	sequence rules	1
3.2.3	Segmentation	1
3.3	**Survival Analytics**	
3.3.1	Kaplan Meier Analysis	2
3.3.2	Parametric Survival Analysis	2
3.3.3	Evaluating Survival Analysis Models	1
3.4	**Text Analytics**	
3.4.1	Overview	1
3.4.2	Text Analytics Methods	1
3.4.3	Text Analytics Metrics	1
3.4.4	Applications	1
3.5	**Social Network Analytics**	
3.5.1	Social network definitions	1
3.5.2	Social network metrics	1
3.5.3	Social network learning	2
3.5.4	Case Study.	1
	Total Lectures	**36**

Course Designers:

1. A.Sheik Abdullah asait@tce.edu
2. A.M.Abirami abiramiam@tce.edu
3. K.V.Uma kvuit@tce.edu

14IS230	**WIRELESS SECURITY**	Category	L	T	P	Credit
		PC	3	1	0	4

Preamble

The course follows the evolution of wireless security, and the underlying principles. The course is designed to educate the purpose of defending systems from unauthorized wireless attacks. This course also discovers the latest security standards and practices in Wireless network.

Prerequisite

- 14IS130 – Network Security

Course Outcomes

On the successful completion of the course, students will be able to

Course Outcomes		**Bloom's Level**
CO1:	Explain the threats to wireless networks, including rogue access points, denial of service (DoS) attacks and client-side threats.	Understand
CO2:	Learn how hackers and auditors alike test wireless networks for vulnerabilities.	Understand
CO3:	Students leave with knowledge they can apply outside the world of Wireless, such as how public key cryptography works.	Apply
CO4:	Explore how an attacker might attempt to subvert and bypass Wireless security measures	Analyze

Mapping with Programme Outcomes

Cos	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11
CO1.	M	L									
CO2.	M	L									
CO3.	S	M	L								
CO4.	S	S	M	L	L			L	M	L	L

S- Strong; M-Medium; L-Low

Assessment Pattern

Bloom's Category	Continuous Assessment Tests			Terminal Examination
	1	2	3	
Remember	20	20	20	20
Understand	80	40	20	20
Apply	-	30	40	40
Analyse	-	10	20	20
Evaluate	-	-	-	-
Create	-	-	-	-

Course Level Assessment Questions

Course Outcome 1 (CO1):

1. Recognize the following attacks and specify the appropriate actions to take to mitigate vulnerability and risk – DOS and DDOS.
2. Define spoofing. Write various types of spoofing.
3. Identify various attacks in wireless networks.

Course Outcome 2 (CO2):

1. Explain in detail about Wired Equivalent Privacy (WEP).
2. Report some of the vulnerabilities susceptible to wireless networks.
3. Report all security issues in GSM.

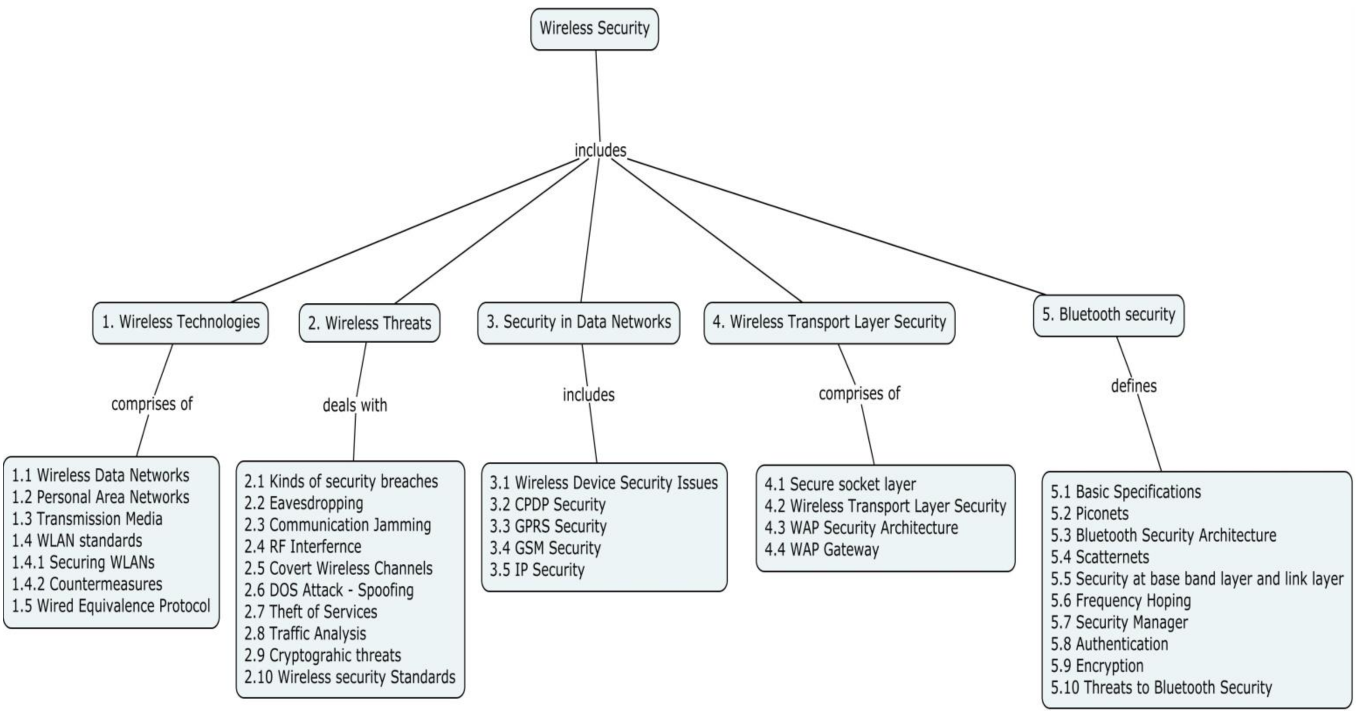
Course Outcome 3 (CO3):

1. For the given network topology, analyze the traffic and find out the safe transmission between nodes.
2. Encrypt the data packets send through Bluetooth using any of the encryption algorithms.
3. Using public key cryptosystems authenticate and encrypt the data transmitted.

Course Outcome 4 (CO4):

- Attained through Assignment

Concept Map



Syllabus

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.

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.

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

Bluetooth security: Basic specifications – Pico nets – Bluetooth security architecture – Scatter nets – Security at the baseband layer and link layer – Frequency hopping – Security manager – Authentication – Encryption – Threats to Bluetooth security introduction to security assessment process

Case studies: Case study 1 – Terrestrial microwave relay systems, Case study 2 – Public safety wireless networks, Case study 3 – Military tactical radio systems, Case study 4 – Satellite communications systems , Case study 5 – Wide Area Wireless Data Services (CDPD, GPRS, etc.), Case study 6 – Wireless LANs (802.11, etc.), Case study 7 – Wireless Metropolitan Area Networks (e.g., 802.16)

Reference Books

1. Nichols and Lekka, “Wireless Security-Models, Threats and Solutions”, Tata McGraw – Hill, New Delhi, 2006.
2. Merritt Maxim and David Pollino, ”Wireless Security”, Osborne/McGraw Hill, New Delhi, 2005.

Course Contents and Lecture Schedule

Module No.	Topic	No. of Lectures
1	**Wireless Technologies**	
1.1	Introduction to wireless technologies	1
1.2	Wireless data networks	1
1.3	Personal Area Networks	1
1.4	Transmission Media	1
1.5	WLAN standards	1
1.5.1	Securing WLANS - Countermeasures	1
1.6	WEP (Wired Equivalence Protocol)	1
2	**Wireless Threats**	
2.1	Kinds of security breaches	1
2.2	Eavesdropping	1
2.3	Communication Jamming	1
2.4	RF interference	1
2.5	Covert wireless channels	1
2.6	DOS attack – Spoofing	1

Module No.	Topic	No. of Lectures
2.7	Theft of services	1
2.8	Traffic Analysis	1
2.9	Cryptographic threats	1
2.10	Wireless security Standards	1
3	**Security in Data Networks**	
3.1	Wireless Device security issues	1
3.2	CDPD security (Cellular Digital Packet Data)	1
3.3	GPRS security (General Packet Radio Service)	1
3.4	GSM (Global System for Mobile Communication) security	1
3.5	IP security	
4	**Wireless Transport Layer Security**	1
4.1	Secure Socket Layer	1
4.2	Wireless Transport Layer Security	1
4.3	WAP Security Architecture	1
4.4	WAP Gateway	1
5	**Bluetooth Security**	
5.1	Basic specifications	1
5.2	Pico nets	1
5.3	Bluetooth security architecture	1
5.4	Scatter nets	1
5.5	Security at the baseband layer and link layer	1
5.6	Frequency hopping	1
5.7	Security manager	1
5.8	Authentication	1
5.9	Encryption	1
5.10	Threats to Bluetooth security introduction to security assessment process	1
6	**Case Studies**	
6.1	Case study 1 – Terrestrial microwave relay systems	2
6.2	Case study 2 – Public safety wireless networks	2
6.3	Case study 3 – Military tactical radio systems	2
6.4	Case study 4 – Satellite communications systems	2
6.5	Case study 5 – Wide Area Wireless Data Services (CDPD, GPRS, etc.)	2
6.6	Case study 6 – Wireless LANs (802.11, etc.)	1
6.7	Case study 7 – Wireless Metropolitan Area Networks (e.g., 802.16)	1
	Total Lectures	**48**

Course Designers:

1. S.Muthuramalingam smrit@tce.edu
2. P.Karthikeyan karthikit@tce.edu
3. T.Manju tmanju@tce.edu

		Category	L	T	P	Credit
14IS270	**DATA ANALYTICS LABORATORY**	PC	0	0	2	1

Preamble

This lab provides the students to explore about various analytics techniques with the intent of performing various functionalities and operations related to data analytics.

Course Outcomes

On the successful completion of the lab, students will be able to

Course Outcomes		Blooms Level
CO1:	Solve different data pre-processing techniques	Apply
CO2:	Develop predictive models for real-time applications	Apply
CO3:	Apply text and social media analytics for unstructured data	Apply

Mapping with Programme Outcomes

COs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11
CO1.	L	L			L				L	L	
CO2.	M	L	L		S			M	M	M	
CO3.	S	M	M	L	S	L		L	M	M	

S- Strong; M-Medium; L-Low

Lab Contents and Schedule

Ex. No	Experiment	No. Of Sessions
1.	Study of tools in data analytics such as Rapid miner, R, Python	2
2.	Data pre-processing	1
3.	Data Classification	1
4.	Data Clustering	1
5.	Implémentation of Prédictive analytics – Multi class Classification	1
6.	Implémentation of Descriptive Analytics – Association rules – sequence rules	1
7.	Text analytics using NLP tools (SNLP/NLTK)	1
8.	Text analytics using R/Python	1
9.	Machine learning techniques for prediction using R/Python	1
10.	Real time data analytics using open source tools like R/Python/HBase	2
	Total Sessions	**12**

Course Designers:

1. A.Sheik Abdullah asait@tce.edu
2. K.V.Uma kvuit@tce.edu
3. A.M.Abirami abiramiam@tce.edu

OUTCOME BASED EDUCATION

CURRICULUM AND DETAILED SYLLABI

FOR

M.E COMPUTER SCIENCE AND INFORMATION SECURITY DEGREE PROGRAMME

PROGRAMME CORE

FOR THE STUDENTS ADMITTED IN THE

ACADEMIC YEAR 2014-15 ONWARDS

THIAGARAJAR COLLEGE OF ENGINEERING
(A Government Aided ISO 9001:2008 certified Autonomous Institution affiliated to Anna University)
MADURAI – 625 015, TAMILNADU

Phone: 0452 – 2482240, 41
Fax: 0452 2483427
Web: www.tce.edu

THIAGARAJAR COLLEGE OF ENGINEERING: MADURAI – 625 015
M.E Degree (Computer Science and Information Security) Program
COURSES OF STUDY
(For the candidates admitted from 2014-2015 onwards)

THIRD SEMESTER

Subject code	Name of the Course	Category	No. of Hours / Week			credits
			L	T	P	
THEORY						
14IS310	Information Security Program Development and Management	PC	3	1	-	4
14ISPX0	Elective-IV	PE	3	1	-	4
14ISPX0	Elective-V	PE	3	1	-	4
PRACTICAL						
14IS340	Project	PC	-	-	12	4
Total			**9**	**3**	**12**	**16**

BS : Basic Science
HSS : Humanities and Social Science
ES : Engineering Science
PC : Program Core
PE : Program Elective
GE : General Elective

L : Lecture
T : Tutorial
P : Practical

Note:

1 Hour Lecture is equivalent to 1 credit
2 Hours Tutorial is equivalent to 1 credit
2 Hours Practical is equivalent to 1 credit

THIAGARAJAR COLLEGE OF ENGINEERING: MADURAI – 625 015

M.E Degree (Computer Science and Information Security) Program

SCHEME OF EXAMINATIONS
(For the candidates admitted from 2014-2015 onwards)

THIRD SEMESTER

S.No.	Sub. code	Name of the Course	Duration of Terminal Exam. in Hrs.	Marks			Minimum Marks for Pass	
				Continuous Assessment *	Terminal Exam **	Max. Marks	Terminal Exam	Total
THEORY								
1	14IS310	Information Security Program Development and Management	3	50	50	100	25	50
2	14ISPX0	Elective-IV	3	50	50	100	25	50
3	14ISPX0	Elective-V	3	50	50	100	25	50
PRACTICAL								
4	14IS340	Project	-	150	150	300	75	150

* Continuous Assessment evaluation pattern will differ from subject to subject and for different tests. This will have to be declared in advance to students. The department will put a process in place to ensure that the actual test paper follow the declared pattern.
** Terminal Examination will be conducted for maximum marks of 100 and subsequently be reduced to 50 marks for the award of terminal examination marks.

14IS310	INFORMATION SECURITY PROGRAM DEVELOPMENT AND MANAGEMENT	Category	L	T	P	Credit
		PC	2	2	0	4

Preamble

This course provides broad understanding of requirements and activities needed to create, manage and maintain a program to implement an information security strategy. The acquired knowledge will be used to manage both the strategic and operational aspects of information security, and to develop business programs implementing effective safeguards to minimize risks to acceptable levels using information security policies.

Prerequisite

- Network Security

Course Outcomes

On the successful completion of the course, students will be able to

Course Outcomes		Bloom's level
CO1:	Explain information security strategy and architectures.	Understand
CO2:	Choose information security standards and procedure to project planning.	Apply
CO3:	Compare the performance of various information security controls.	Analyze
CO4:	Determine the efficiency of the information security metrics.	Apply
CO5:	Examine appropriate techniques to solve problems in the discipline of information security management	Apply

Mapping with Programme Outcomes

COs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11
CO1	L										
CO2	S	M	L				S		M		
CO3	S	S	M								
CO4	S	M	L				S				
CO5	S	M	M						L	M	M

S- Strong; M-Medium; L-Low

Assessment Pattern

Bloom's Category	Continuous Assessment Tests			Terminal Examination
	1	2	3	
Remember	20	20	20	20
Understand	50	30	20	20
Apply	30	50	50	50
Analyse	0	0	10	10
Evaluate	0	0	0	0
Create	0	0	0	0

Course Level Assessment Questions

Course Outcome 1 (CO1):

1. Explain in detail about the purpose and elements of different types of security architectures.
2. Write about the integration policy and governance process with an example.
3. What are the factors affecting Inter departmental collaboration?

Course Outcome 2 (CO2):

1. How will you adapt information security standards and procedures in project plan? Explain.
2. Illustrate the oracle supplier information and physical security standards in detail.
3. Rewrite about the third party risks that may arise in an organization with example.

Course Outcome 3 (CO3):

1. Explain about the various Information security technologies and its purposes.
2. Illustrate how will you provide security culture and secure environment while developing a project.
3. Explain about the various kinds of controls and its uses in detail.

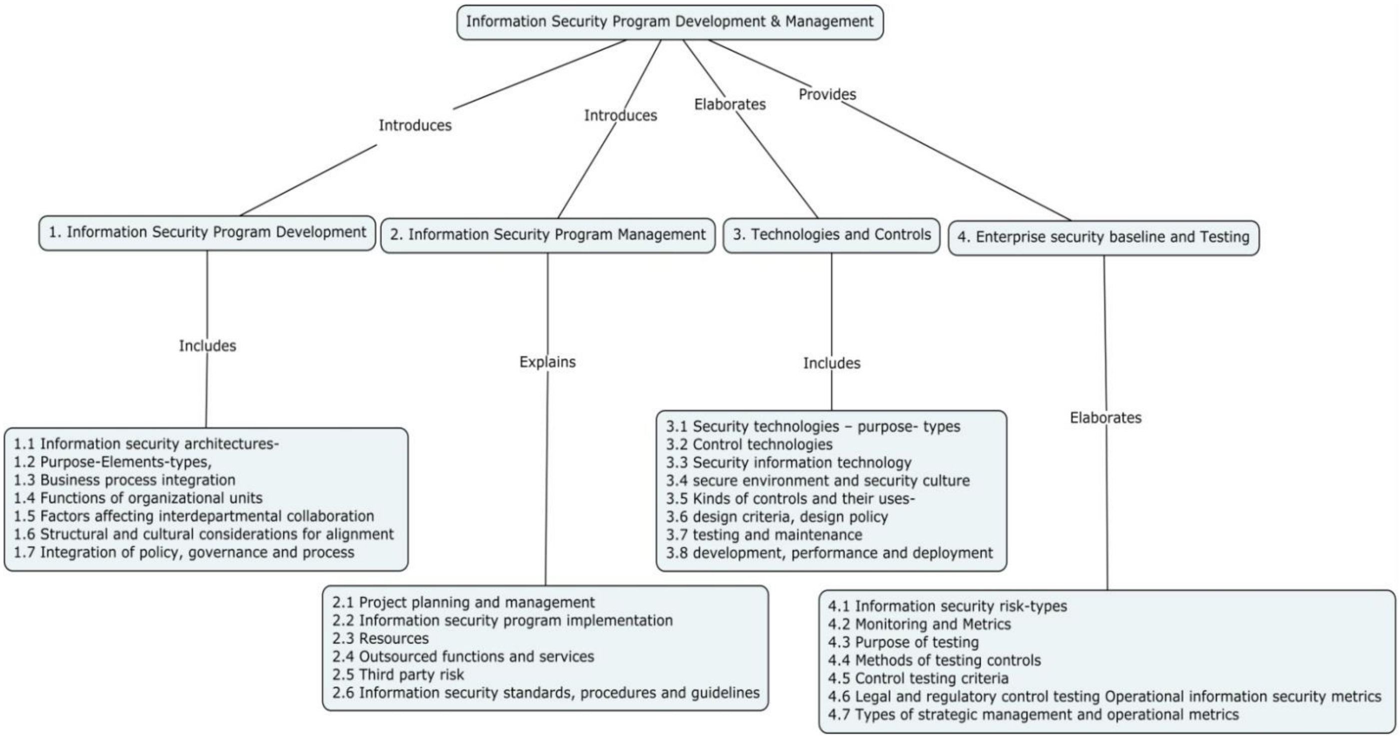
Course Outcome 4 (CO4):

1. Explain in detail about the various types of information security risks.
2. Illustrate the purpose of testing and the methods of testing controls.
3. Explain in detail about the various types of strategic management and operational risks.

Course Outcome 5 (CO5):

1. Explain about Information Security Management in healthcare industry.
2. Explain the ways of Protecting high tech trade secrets
3. Illustrate the purpose of Outsourcing Security with example.

Concept Map



Syllabus

Information Security Program Development - Information security architectures for organizations -Purpose-Elements-types, Business process integration- Functions of organizational units - Factors affecting interdepartmental collaboration -Structural and cultural considerations for alignment - Integration of policy, governance and process

Information Security Program Management - Project planning and management -Information security program implementation – Resources -Outsourced functions and services -Third party risk – Information security standards, procedures and guidelines.

Technologies and Controls - Security technologies – purpose- types, Control technologies**,** Security information technology - secure environment and security culture. Kinds of controls and their uses-design criteria -design policy -testing and maintenance -development, performance and deployment

Enterprise security baseline and Testing - Information security risk-types- monitoring and metrics, Purpose of testing -Methods of testing controls -Control testing criteria -Legal and regulatory control testing Operational information security metrics, Types of strategic management and operational metrics.

Case study - Business case for Information Security- Information Security Management in healthcare industry- Protecting high tech trade secrets- Outsourcing Security.

Reference Books

1 Micki Krause, Harold F.Tripton, “Information Security Management Handbook”, Auerbach Publications, Sixth Edition, 2012

2. The Little Black Book of Computer Security, Dubin, Joel, Penton Media Inc. USA, 2nd *Edition*, 2008.
3. Axelrod, C. Warren; Outsourcing Information Security, Artech House, USA, 2004

Course Contents and Lecture Schedule

Module No.	Topic	No. of Lectures
1.	**Information Security Program Development**	
1.1	Information security architectures	1
1.2	Purpose-Elements-types	1
1.3	Business process integration	1
1.4	Functions of organizational units	1
1.5	Factors affecting interdepartmental collaboration	1
1.6	Structural and cultural considerations for alignment	1
1.7	Integration of policy, governance and process	1
2.	**Information Security Program Management**	
2.1	Project planning and management	1
2.2	Information security program implementation	2
2.3	Resources	1
2.4	Outsourced functions and services	1
2.5	Third party risk	1
2.6	Information security standards, procedures and guidelines	1
3.	**Technologies and Controls**	
3.1	Security technologies – purpose- types	1
3.2	Control technologies	1
3.3	Security information technology	1
3.4	secure environment and security culture	1
3.5	Kinds of controls and their uses	1
3.6	Design criteria -design policy	1
3.7	Testing and maintenance	1
3.8	Development, performance and deployment	2
4.	**Enterprise security baseline and Testing**	
4.1	Information security risk-types	1
4.2	Monitoring and Metrics	1
4.3	Purpose of testing	1
4.4	Methods of testing controls	2
4.5	Control testing criteria	1
4.6	Legal and regulatory control testing Operational information security metrics	1
4.7	Types of strategic management and operational metrics	1
5.	**Case study**	
5.1	Business case for Information Security	1
5.2	Information Security Management in healthcare industry	1

Module No.	Topic	No. of Lectures
5.3	Protecting high tech trade secret	1
5.4	Outsourcing Security	1
	Total Lectures	**36**

Course Designers:

1. Ms.S.Sujitha sujithait@tce.edu
2. Ms.S.Pudumalar spmit@tce.edu
3. Ms.Raja Lavanya rlit@tce.edu

THIAGARAJAR COLLEGE OF ENGINEERING: MADURAI – 625 015
M.E Degree (Computer Science and Information Security) Program
COURSES OF STUDY
(For the candidates admitted from 2014-2015 onwards)

FOURTH SEMESTER

Subject code	Name of the Course	Category	No. of Hours / Week			credits
			L	T	P	
PRACTICAL						
14IS410	Project	PC	-	-	12	12
Total			**-**	**-**	**12**	**12**

BS : Basic Science
HSS : Humanities and Social Science
ES : Engineering Science
PC : Program Core
PE : Program Elective
GE : General Elective

L : Lecture
T : Tutorial
P : Practical

Note:

1 Hour Lecture is equivalent to 1 credit
2 Hours Tutorial is equivalent to 1 credit
2 Hours Practical is equivalent to 1 credit

THIAGARAJAR COLLEGE OF ENGINEERING: MADURAI – 625 015

M.E Degree (Computer Science and Information Security) Program

SCHEME OF EXAMINATIONS

(For the candidates admitted from 2014-2015 onwards)

FOURTH SEMESTER

S.No.	Sub. code	Name of the Course	Duration of Terminal Exam. in Hrs.	Marks			Minimum Marks for Pass	
				Continuous Assessment *	Terminal Exam **	Max. Marks	Terminal Exam	Total
PRACTICAL								
1	14IS410	Project	-	150	150	300	75	150

* Continuous Assessment evaluation pattern will differ from subject to subject and for different tests. This will have to be declared in advance to students. The department will put a process in place to ensure that the actual test paper follow the declared pattern.

** Terminal Examination will be conducted for maximum marks of 100 and subsequently be reduced to 50 marks for the award of terminal examination marks.

CURRICULUM AND DETAILED SYLLABI

FOR

M.E DEGREE (COMPUTER SCIENCE AND INFORMATION SECURITY) PROGRAMME

PROGRAMME ELECTIVES

FOR THE STUDENTS ADMITTED IN THE

ACADEMIC YEAR 2014-15 ONWARDS

THIAGARAJAR COLLEGE OF ENGINEERING
(A Government Aided ISO 9001:2008 certified Autonomous Institution affiliated to Anna University)
MADURAI – 625 015, TAMILNADU

Phone: 0452 – 2482240, 41
Fax: 0452 2483427
Web: www.tce.edu

List of Electives

S.No	ELECTIVE CODE	PROGRAM ELECTIVE
1.	14ISPA0	Multimedia Security
2.	14ISPB0	Information Theory and Coding
3.	14ISPC0	Machine Learning
4.	14ISPD0	Web Mining
5.	14ISPE1	Ethical Hacking and Cyber Forensics
6.	14ISPF1	Cloud and Security
7.	14ISPG0	IT Audit and Control

		Category	L	T	P	Credit
14ISPA0	**MULTIMEDIA SECURITY**	PE	3	1	0	4

Preamble

With the tremendous growth of the Internet and computer technologies, and the wide usage of multimedia content such as audio, image and video data, the protection and authentication of multimedia contents is becoming increasingly important to industry and government sectors, as well as for individual personal usage. Protection of ownership and authentication of multimedia contents and documents have also attracted significant attention in the digital arena through the application of digital watermarking and digital rights management technologies. This course will provide an introductory background to various digital security technologies currently used in different applications for multimedia contents and documents.

Prerequisite

- 14IS120: Cryptography
- 14IS130: Network Security
- 14IS140: Network Technologies

Course Outcomes

On the successful completion of the course, students will be able to

Course Outcomes		Bloom's Level
CO1:	Demonstrate a systematic understanding of multimedia computing and main security problems involving multimedia data.	Understand
CO2:	Perform encryption of images and videos using selective encryption, full encryption and syntax compliant encryption approaches.	Apply
CO3:	Compare and contrast different watermarking techniques for image files in frequency and spatial domain.	Understand
CO4:	Elaborate digital steganography and steganalysis techniques for images and text documents.	Understand
CO5:	Comprehend the various types of attacks against multimedia encryption and watermarking algorithms.	Understand
CO6:	Perform encryption of multimedia files and generate watermarks for image files and implement steganographic algorithms for images/ video files and analyze the strength through various steganalysis mechanisms.	Apply

Mapping with Programme Outcomes

COs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11
CO1.	M	M									
CO2.	S	M									
CO3.	M	M									
CO4	M	M									
CO5.	M	L									
CO6	S	M	S	L	M					L	L

S- Strong; M-Medium; L-Low

Assessment Pattern

Bloom's Category	Continuous Assessment Tests			Terminal Examination
	1	2	3	
Remember	20	20	20	20
Understand	50	50	50	50
Apply	30	30	30	30
Analyze	0	0	0	0
Evaluate	0	0	0	0
Create	0	0	0	0

Attainment of Course Outcomes 6 is evaluated through practical assignments.

Course Level Assessment Questions

Course Outcome 1 (CO1):

1. Identify the main forms of media storage and distribution mechanisms.
2. Explain the various intellectual property rights.
3. Enlist some of the security applications of multimedia.

Course Outcome 2 (CO2):

1. Highlight some of the advantages of selective encryption over full encryption.
2. Elaborate the procedure for semi fragile crypto hash based image authentication.
3. Identify the special requirements for video authentication.

Course Outcome 3 (CO3):

1. Explain the procedure for Spread Spectrum watermarking.
2. Differentiate copy deterrence and copy protection.
3. Elaborate the steps with reference to the buyer seller watermarking protocol:
   a. Watermark Generation
   b. Watermark Insertion
   c. Copy right violator identification
   d. Dispute Resolution

Course Outcome 4 (CO4):

1. List some of the image metrics that can be used for steganalyis.
2. Discuss the application of support vector machines for steganalysis
3. Develop the pseudo code for Least Significant Bit method of steganography.

Course Outcome 5 (CO5):

1. Describe the various image processing attacks on watermarks.
2. Differentiate statistical attack and error concealment attack with respect to image encryption.
3. Describe the various types of attacks for stegnography algorithms.

Course Outcome 6 (CO6): (Practical Assignments)

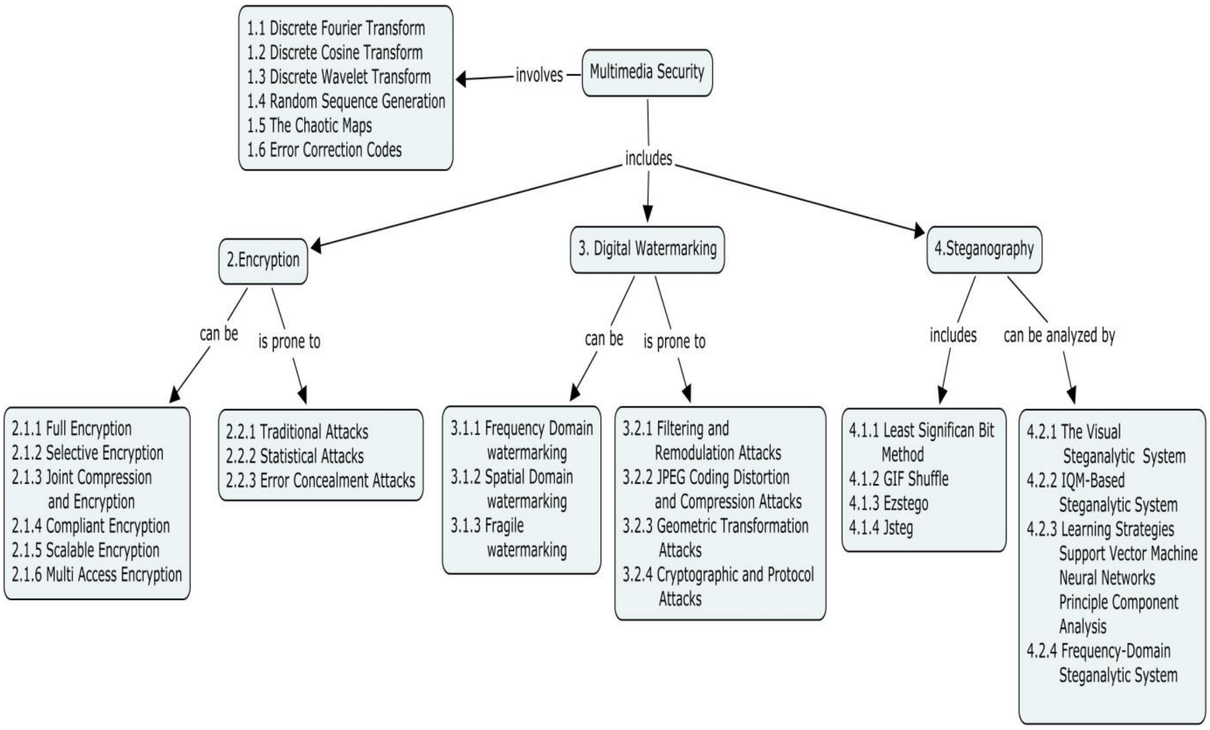
1. Generate an image format converter which reads raw images (e.g., PPM format) and writes them as BMP format. The generated BMP file has to be readable by general image viewer.

Perform 8x8 DCT transform on the images. Try the following operations and then perform inverse DCT transform. Compare the differences (e.g., show PSNR values)./ Leave only the DC values. Delete all AC values. Leave the DC value and 5 AC values (in the zigzag order) in each block.

a. Quantize the DCT coefficients using the standard JPEG quantization table.
b. Perform encryption on the DCT coefficients of images by the following shuffling methods and then perform inverse DCT on them. Observe the results. You can use any encryption method (e.g., randomly generate a look-up table for shuffling).
c. Encrypting the DC coefficients of blocks. Don't change the AC coefficients.
d. Encrypting the AC coefficients within each block. Any shuffling method can be used.
e. Encrypting the AC coefficients based on the format compliant encryption.

2. Implement the LSB-based watermarking methods and change the least significant bits in the spatial domain.
   a. Change the least significant bits in the Block-base DCT domain before quantization.
   b. Change the least significant bits in the Block-based DCT-domain after quantization.

Concept Map



Syllabus

Introduction to Multimedia - Image, Video and Audio Formats and Standards, and Digital Rights Management Mathematical Preliminaries - Discrete Fourier Transform, Discrete Cosine Transform, Discrete Wavelet Transform ,Random Sequence Generation, The Chaotic Maps , Error Correction Codes.

Multimedia Encryption – Requirements and Applications **Approaches** – Full Encryption, Selective Encryption, Joint Compression and Encryption, Syntax-Compliant Encryption, Scalable Encryption and Multi-Access Encryption. **Attacks** – Traditional Attacks, Statistical Attack, Error concealment attack.

Digital Water marking – Requirements and Applications, **Watermarking Algorithms**- Spatial-Domain Watermarking - Substitution and Additive Watermarking. Frequency-Domain Watermarking - Substitution and Multiplicative Watermarking, Watermarking Based on

Vector Quantization, Fragile Watermarking - Block-Based and Hierarchical Block-Based watermarking. **Water Marking Protocols** - A Buyer-Seller Watermarking Protocol, Extensions of Watermarking Protocols, Protocols for Secure Computation **Attacks** - Filtering, Remodulation, JPEG Coding Distortion and JPEG 2000 Compression, Geometric Transformation -Image Scaling, Rotation, Image Clipping, Linear Transformation, Bending, Warping and Perspective Projection, Cryptographic attacks and Protocol attacks, Watermarking Tools.

Steganography – Requirements and Applications, **Types**– Text, Audio, Video, Linguistic and Network steganography **Algorithms** – Least Significant Method, GIFshuffle, EzStego, Jsteg, Steganographic Tools **Steganalysis -** Statistical Properties of Images, The Visual Steganalytic System, IQM-Based Steganalytic System, Learning Strategies- Support Vector Machine, Neural Networks, Principle Component Analysis, Frequency-Domain Steganalytic System.

Reference Books

1. Cox, Miller, Bloom, Fridrich, and Kalker, " Digital Watermarking and Steganography", 2nd Edition, 2008

Wenjun Zeng, Heather Yu, Ching-Yung Lin, "Multimedia Security Technologies for Digital Rights Management", Elsevier, 2006

Borko Furht, Darko Kirovski "Multimedia Security Handbook", CRC Press, 2004

Course Contents and Lecture Schedule

Module No.	Topic	No. of Lectures
0	**Introduction to Multimedia**	
0.1	Image, Video and Audio Formats and Standards	2
0.2	Digital Rights Management	1
1	**Mathematical Preliminaries**	
1.1	Discrete Fourier Transform	1
1.2	Discrete Cosine Transform	
1.3	Discrete Wavelet Transform	2
1.4	Random Sequence Generation	
1.5	Chaotic Maps	2
1.6	Error Correction Codes	
2 2.0	**Multimedia Encryption** Requirements and Applications	1
2.1	**Encryption Approaches**	
2.1.1 2.1.2	Full Encryption Selective Encryption	2
2.1.3 2.1.4	Joint Compression and Encryption Syntax-Compliant Encryption	1
2.1.5 2.1.6	Scalable Encryption Multi-Access Encryption	1
2.2 2.2.1 2.2.2 2.2.3	**Attacks** Traditional Attacks Statistical Attack Error concealment attack	2
3 3.1.1	**Digital Watermarking Algorithms :** Requirements and applications **Spatial-Domain Watermarking :** Substitution and Additive Watermarking	2
3.1.2	**Frequency-Domain Watermarking** Substitution and Multiplicative Watermarking	2

Module No.	Topic	No. of Lectures
	Watermarking Based on Vector Quantization	
3.1.3	**Fragile Watermarking** Block-Based and Hierarchical Block-Based watermarking	1
3.2 3.2.1 3.2.2	Attacks Filtering and Remodulation JPEG Coding Distortion and JPEG 2000 Compression	2
3.2.3	Geometric Transformation -Image Scaling, Rotation, Image Clipping, Linear Transformation, Bending, Warping and Perspective Projection	2
3.2.4	Cryptographic attacks and Protocol attacks	2
3.3	**Water Marking Protocols** A Buyer-Seller Watermarking Protocol Extensions of Watermarking Protocols Protocols for Secure Computation	2
3.4	Watermarking Tools.	2
4.0	**Steganography –** Requirements and Applications **Types**– Text, Audio, Video, Linguistic and Network steganography	2
4.1 4.1.1 4.1.2	**Steganography Algorithms** Least Significant Method GIFshuffle	2
4.1.3 4.1.4	EzStego Jsteg	2
4.2	Steganalysis - Statistical Properties of Images	1
4.2.1	The Visual Steganalytic System	2
4.2.2	IQM-Based Steganalytic System	2
4.2.3	Learning Strategies Support Vector Machine Neural Networks Principle Component Analysis	3
4.2.4	Frequency-Domain Steganalytic System	2
4.3	Steganographic Tools	2
	Total Lectures	**48**

Course Designers:

1. C.Jeyamala jeyamala@tce.edu
2. M.Thangavel mtit@tce.edu

		Category	L	T	P	Credit
14ISPB0	**INFORMATION THEORY AND CODING**	PE	3	1	0	4

Preamble

The objective of this course is to introduce the principles of information theory and study how information is measured in terms of probability and entropy, and the relationships among conditional and joint entropies; how these are used to calculate the capacity of a communication channel, with and without noise; coding schemes, including error correcting codes; how discrete channels and measures of information generalize to their continuous forms.

Prerequisite

- Nil

Course Outcomes

On the successful completion of the course, students will be able to

Course Outcomes		**Bloom's Levels**
CO1:	Explain the fundamental concepts of probability, Entropy, Information Theory and Error Correction	Understand
CO2:	Explore the application of source coding, and error control methods for Digital Data Streams.	Apply
CO3:	Analyze the various concepts of Source coding and Error Control methods.	Analyze
CO4:	Apply Theorems and Analyze the performance of communication channels.	Analyze

Mapping with Programme Outcomes

COs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11
CO1	S										
CO2				M							
CO3		M	L	M							
CO4		M	L	M							

S- Strong; M-Medium; L-Low

Assessment Pattern

Bloom's Category	Continuous Assessment Tests			Terminal Examination
	1	2	3	
Remember	20	10	0	10
Understand	20	20	30	30
Apply	60	40	50	40
Analyze	0	30	20	20
Evaluate	0	0	0	0
Create	0	0	0	0

Course Level Assessment Questions

Course Outcome 1 (CO1):

1. Identify the shortest possible code length, in bits per average symbol, that could be achieved for a six-letter alphabet whose symbols have the following probability distribution?
{ 1/2, 1/4, 1/8, 1/16, 1/32, 1/32 }.
2. Infer From the Following: Suppose that ravens are black with probability 0.6, that they are male with probability 0.5 and female with probability 0.5, but that male ravens are 3 times more likely to be black than are female ravens. If you see a non-black raven, what is the probability that it is male? How many bits worth of information are contained in a report that a non-black raven is male?Rank-order for this problem, from greatest to least, the following uncertainties: (i) uncertainty about color; (ii) uncertainty about gender; (iii) uncertainty about colour, given only that a raven is male; (iv) uncertainty about gender, given only that a raven is non-black.
3. Explain the entropy H, in bits, of the following source alphabet whose letters have the probabilities shown?

A	B	C	D
1/4	1/8	1/2	1/8

4. Infer from the Following: Suppose that women who live beyond the age of 80 outnumber men in the same age group by three to one. How much information, in bits, is gained by learning that a person who lives beyond 80 is male?

Course Outcome 2 (CO2):

1. An error-correcting Hamming code uses a 7 bit block size in order to guarantee the detection, and hence the correction, of any single bit error in a 7 bit block. Show how many bits are used for error correction, and how many bits for useful data? If the probability of a single bit error within a block of 7 bits is p = 0.001, what is the probability of an error correction failure, and what event would cause this?
2. Illustrate the Huffman codes for equal probabilities.
3. Illustrate the Source Coding theorem.
4. Consider (3,1,2) convolutional code with g(1) = (110), g(2) = (101) and g(3) = (111):
   (i) Sketch the encoder block diagram.
   (ii) Discover the generator matrix.
   (iii) Discover the code word corresponding to the information sequence (11101) using time domain approach
5. Define BCH code and brief about Reed-Solomon code.

Course Outcome 3 (CO3):

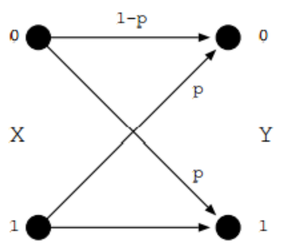
CO3 is attained through Assignment 1

Assignment I Details

1. Identify a suitable problem.
2. Analyze the problem(Requirements and Functionality)
3. Select suitable Error Correction Methods
4. Implement and submit the results and findings.

Course Outcome 4 (CO4):

1.



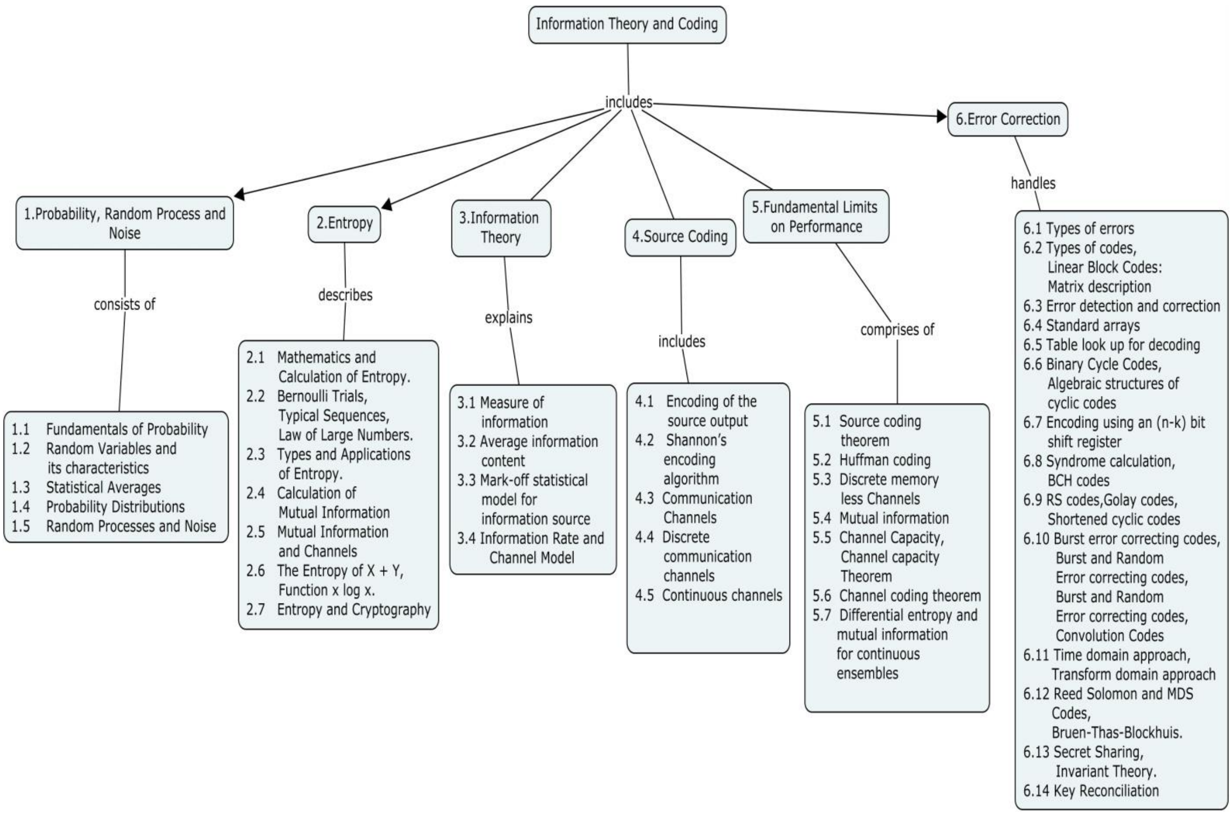
For the binary symmetric channel with transition probability p, derive the channel capacity. Sketch a graph of the channel capacity against the transition probability.

2. Model a symmetric (7,4) cyclic code using the generator polynomial $g(x)= x^3+x+1$. What are the error correcting capabilities of this code? For the received word 1101100, determine the transmitted codeword.

3. Analyze differential entropy to compare the randomness of random variables.

4. Consider a noiseless analog communication channel whose bandwidth is 10,000 Hertz. A signal of duration 1 second is received over such a channel. We wish to represent this continuous signal exactly, at all points in its one-second duration, using just a finite list of real numbers obtained by sampling the values of the signal at discrete, periodic points in time. Infer the length of the shortest list of such discrete samples required in order to guarantee that we capture all of the information in the signal and can recover it exactly from this list of samples?

Concept Map



Syllabus

Probability, Random process and Noise: Fundamentals of Probability-Random Variables and its characteristics-Statistical Averages-Probability Distributions-Random Processes and Noise.

Entropy: Mathematics and Calculation of Entropy-Bernoulli Trials, Typical Sequences, Law of Large Numbers-Types and Applications of Entropy-Calculation of Mutual Information-Mutual Information and Channels-The Entropy of X + Y, Function x log x-Entropy and Cryptography.

Information Theory: Measure of information-Average information content-Mark-off statistical model for information source-Information Rate and Channel Model.

Source Coding: Encoding of the source output-Shannon's encoding algorithm-Communication Channels-Discrete communication channels-Continuous channels.

Fundamental Limits on Performance: Source coding theorem-Huffman coding-Discrete memory less Channels-Mutual information-Channel Capacity, Channel capacity Theorem-Channel coding theorem-Differential entropy and mutual information for continuous ensembles.

Introduction to Error Control Coding: Types of errors-Types of codes, Linear Block Codes: Matrix description-Error detection and correction-Standard arrays-Table look up for decoding-Binary Cycle Codes, Algebraic structures of cyclic codes-Encoding using an (n-k) bit shift register-Syndrome calculation, BCH codes-RS codes, Golay codes, Shortened cyclic codes-Burst error correcting codes, Burst and Random Error correcting codes, Burst and Random Error correcting codes, Convolution Codes-Time domain approach, Transform domain approach-Reed Solomon and MDS Codes, Bruen-Thas-Blockhuis-Secret Sharing, Invariant Theory-Key Reconciliation.

Text Book

1. Ranjan Bose, "Information Theory, Coding and Cryptography",Tata McGraw-Hill Education, 2008
2. Arijit Saha, NilotPal Manna, Surajit Mandal, "Information Theory, Coding and Cryptography", Pearson Education , 2013

References

1. K Sayood, "Introduction to Data Compression" 3/e, Elser 2006.
2. S Gravano, "Introduction to Error Control Codes", Oxford University Press 2007.

Course Contents and Lecture Schedule

Module No.	Topic	No of Lectures
1	**Probability, Random process and Noise**	
1.1	Fundamentals of Probability	1
1.2	Random Variables and its characteristics	
1.3	Statistical Averages	1
1.4	Probability Distributions	1
1.5	Random Processes and Noise	1
2	**Entropy**	
2.1	Mathematics and Calculation of Entropy.	1

2.2	Bernoulli Trials, Typical Sequences, Law of Large Numbers.	2
2.3	Types and Applications of Entropy.	1
2.4	Calculation of Mutual Information	1
2.5	Mutual Information and Channels	1
2.6	The Entropy of X + Y, Function x log x.	2
2.7	Entropy and Cryptography.	2
3	**Information Theory**	
3.1	Measure of information	1
3.2	Average information content	
3.3	Mark-off statistical model for information source	1
3.4	Information Rate and Channel Model	1
4	**Source Coding**	
4.1	Encoding of the source output	1
4.2	Shannon's encoding algorithm	
4.3	Communication Channels	1
4.4	Discrete communication channels	1
4.5	Continuous channels	1
5	**Fundamental Limits on Performance**	
5.1	Source coding theorem	1
5.2	Huffman coding	1
5.3	Discrete memory less Channels	2
5.4	Mutual information	1
5.5	Channel Capacity, Channel capacity Theorem	2
5.6	Channel coding theorem	1
5.7	Differential entropy and mutual information for continuous ensembles	2
6	**Introduction to Error Control Coding**	
6.1	Types of errors	2
6.2	Types of codes, Linear Block Codes: Matrix description	
6.3	Error detection and correction	3
6.4	Standard arrays	
6.5	Table look up for decoding	
6.6	Binary Cycle Codes, Algebraic structures of cyclic codes	2
6.7	Encoding using an (n-k) bit shift register	1
6.8	Syndrome calculation, BCH codes	
6.9	RS codes, Golay codes, Shortened cyclic codes	3
6.10	Burst error correcting codes, Burst and Random Error correcting codes, Burst and Random Error correcting codes, Convolution Codes	
6.11	Time domain approach, Transform domain approach	2
6.12	Reed Solomon and MDS Codes, Bruen-Thas-Blockhuis.	3
6.13	Secret Sharing,Invariant Theory.	
6.14	Key Reconciliation	
Total Lectures		**48**

Course Designers

1. C. V. Nisha Angeline nishaangeline@gmail.com
2. M. Ayswharya Devi ayswharyadevi@gmail.com

14ISPCO	**MACHINE LEARNING**	Category	L	T	P	Credit
		PE	3	1	0	4

Preamble

The objective of the course is to make the students to learn the concepts behind several machine learning algorithms and gain practical learning to apply for the above in real world problems.

Prerequisite

- Nil

Course Outcomes

On the successful completion of the course, students will be able to

Course Outcomes		**Bloom's Levels**
CO1:	Comprehend the basic concepts and techniques of Machine Learning	Understand
CO2:	Analyse the difference between various leaning techniques	Analyze
CO3:	Apply the machine learning techniques to real world problems	Apply

Mapping with Programme Outcomes

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	L	L	M									
CO2	L	L	M									
CO3	S	M	L	L	M							**L**

S- Strong; M-Medium; L-Low

Assessment Pattern

Bloom's Category	**Continuous Assessment Tests**			**Terminal Examination**
	1	**2**	**3**	
Remember	20	20	0	20
Understand	60	20	20	20
Apply	20	40	80	30
Analyse	10	20	40	30
Evaluate	0	0	0	0
Create	0	0	0	0

Course Level Assessment Questions

Course Outcome 1 (CO1):

1. Compare supervised and unsupervised learning
2. List the features of EM Algorithm
3. Define Occam learning.

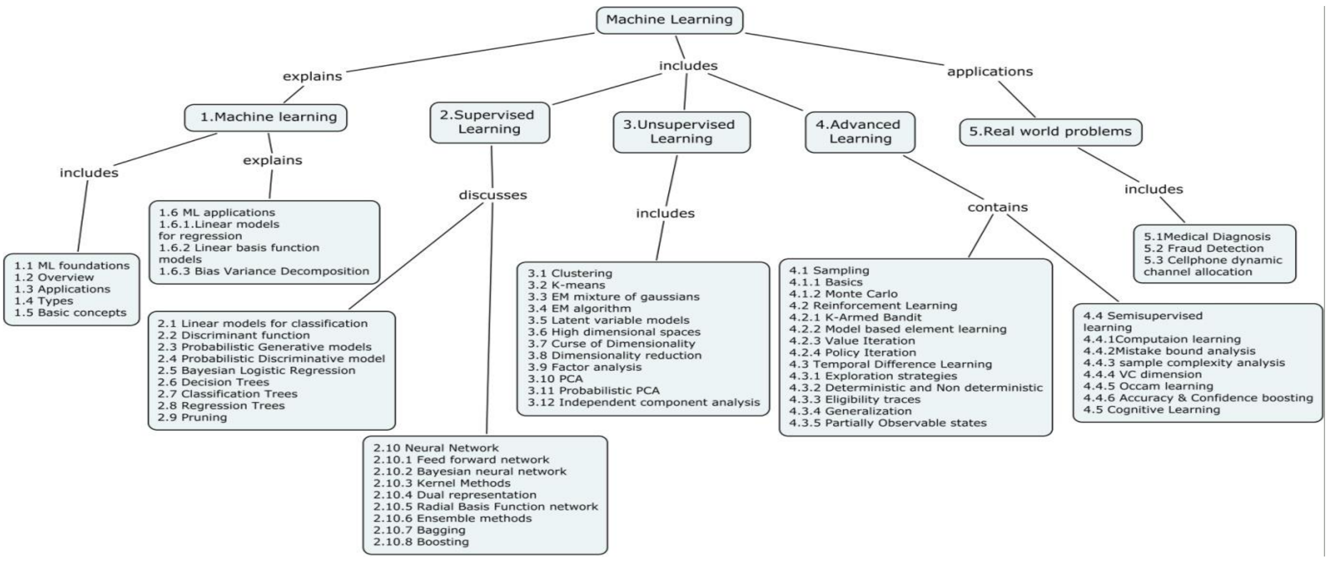
Course Outcome 2 (CO2):

1. How unlabeled data be helpful for supervised learning, justify with example
2. List the ways to deal the over fitting in neural networks?
3. Summarise the RBF features over other network

Course Outcome 3 (CO3):

1. What is the relationship between different learning algorithms, and which should be used when?
2. Can machine learning theories and algorithms help explain human learning?
3. Apply the RL technique for the 4 elevators in a ten story building. if passengers on several floors have requested pickups, which should be served first? If there are no pickup requests, how should the elevators distribute themselves to await the next request? Apply the reinforcement learning for finding the optimal strategy for the elevator to satisfy the commercial dispatching needs of people waiting to be less

Concept Map



Syllabus

Machine Learning – ML Foundations –Overview – applications - Types of machine learning - Basic concepts in machine learning - Examples. ML Applications – Linear Models for Regression - Linear Basis Function Models - The Bias-Variance Decomposition.

Supervised Learning - Linear Models for Classification - Discriminant Functions - Probabilistic Generative Models - Probabilistic Discriminative Models - Bayesian Logistic Regression. Decision Trees – Classification Trees- Regression Trees - Pruning. Neural Networks -Feed-forward Network Functions -Bayesian Neural Networks - Kernel Methods - Dual Representations - Radial Basis Function Networks. Ensemble methods- Bagging- Boosting.

Unsupervised Learning - Clustering- K-means - EM - Mixtures of Gaussians - The EM Algorithm in General -Model selection for latent variable models - high-dimensional spaces -- The Curse of Dimensionality –Dimensionality Reduction - Factor analysis - Principal Component Analysis - Probabilistic PCA- Independent components analysis

Advanced Learning - Sampling – Basic sampling methods – Monte Carlo. Reinforcement Learning- K-Armed Bandit- Elements - Model-Based Learning- Value Iteration- Policy Iteration. Temporal Difference Learning- Exploration Strategies- Deterministic and Non-deterministic Rewards and Actions- Eligibility Traces- Generalization- Partially Observable States. Semi - Supervised Learning. Computational Learning Theory - Mistake bound analysis, sample complexity analysis, VC dimension. Occam learning, accuracy and confidence boosting –Cognitive learning.

Case Studies of Real World Problems on Medical Diagnosis, Fraud Detection & Cell phone Dynamic channel allocation.

Text Book

1. Christopher Bishop, “Pattern Recognition and Machine Learning” Springer, 2006.
2. Tom Mitchell, "Machine Learning", McGraw-Hill, 1997.

Reference Books

1. Ethem Alpaydin, “Introduction to Machine Learning”, Prentice Hall of India, 2005.
2. Kevin P. Murphy, “Machine Learning: A Probabilistic Perspective”, MIT Press, 2012.
3. Hastie, Tibshirani, Friedman, “The Elements of Statistical Learning” (2nd ed)., Springer, 2008.
4. Stephen Marsland, “Machine Learning –An Algorithmic Perspective”, CRC Press, 2009

Course Contents and Lecture Schedule

Module No.	Topic	No. of Lectures
1	**Machine Learning**	
1.1	ML foundation	
1.2	Overview	1
1.3	Applications	3
1.4	Types of Machine learning	
1.5	Basic Concepts	2
1.6	**ML Applications**	
1.6.1	Linear Models for Regression	2
1.6.2	Linear Basis Function Models	
1.6.3	The Bias-Variance Decomposition	
2	**Supervised Learning**	
2.1	Linear Models for Classifications	2
2.2	Discriminant Functions	1
2.3	Probabilistic Generative Models	
2.4	Probabilistic Discriminative Models	
2.5	Bayesian Logistic Regression	2
2.6	Decision Trees	
2.7	Classification Trees	1
2.8	Regression Trees	
2.9	Pruning	
2.10	**Neural Network**	
2.10.1	Feed-forward Network Functions	2
2.10.2	Bayesian Neural Networks	2
2.10.3	Kernel Methods	
2.10.4	Dual Representations	1
2.10.5	Radial Basis Function Networks	
2.10.6	Ensemble methods	1

Module No.	Topic	No. of Lectures
2.10.7	Bagging	
2.10.8	Boosting	
3	**Unsupervised Learning**	
3.1	Clustering	1
3.2	K-means	2
3.3	EM Mixtures of Gaussians	
3.4	EM Algorithm	1
3.5	Latent variable models	
3.6	High-dimensional spaces	2
3.7	Curse of Dimensionality	
3.8	Dimensionality Reduction	1
3.9	Factor analysis	1
3.10	Principal Component Analysis	1
3.11	Probabilistic PCA	
3.12	Independent components analysis	1
4	**Advanced Learning**	
4.1	Sampling	1
4.1.1	Basic sampling methods	1
4.1.2	Monte Carlo	1
4.2	**Reinforcement Learning**	
4.2.1	K-Armed Bandit	
4.2.2	Model based element learning	1
4.2.3	Value Iteration	
4.3	Temporal Difference Learning	1
4.3.1	Exploration Strategies	
4.3.2	Deterministic & Non-deterministic Rewards and Actions	2
4.3.3	Eligibility Traces	
4.3.4	Generalization	1
4.3.5	Partially Observable States	
4.4	**Semi-supervised Learning**	
4.4.1	Computational Learning Theory	2
4.4.2	Mistake bound analysis	2
4.4.3	Sample complexity analysis	
4.4.4	VC dimension	
4.4.5	Occam learning	
4.4.6	Accuracy and confidence boosting	1
4.5	Cognitive learning	2
5	**Case studies of Real World Problems**	
5.1	Medical Diagnosis	1
5.2	Fraud Detection	1
5.3	Cell phone Dynamic channel allocation	
Total Lectures		**48**

Course Designers:

1. D.Tamilselvi dtamilselvi@tce.edu
2. R.Suganya rsuganya@tce.edu

14ISPD0	**WEB MINING**	Category	L	T	P	Credit
		PE	3	1	0	4

Preamble

Web mining aims to discover useful information or knowledge from Web hyperlinks, page contents, and usage logs. Based on the primary kinds of data used in the mining process, the students will be able to discover knowledge from hyperlinks, extract useful information/knowledge from Web page contents and mines user access patterns from usage logs, which record clicks made by every user.

Prerequisite

- Nil.

Course Outcomes

On the successful completion of the course, students will be able to

Course Outcomes		Bloom's Level
CO1:	Comprehend the typical Web Log Structure	Understand
CO2:	Illustrate the Web Content Mining by web crawlers	Apply
CO3:	Demonstrate Web structure Mining using Page Rank and HITS	Apply
CO4:	Experiment the Web usage mining using web log analysis tools	Analyze

Mapping with Programme Outcomes

COs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11
CO1	L										
CO2	M	L			L			M	L		
CO3	M	L			L			M	L		
CO4	S	M	L	L	L	L	L	M	L	L	L

S- Strong; M-Medium; L-Low

Assessment Pattern

Bloom's Category	Continuous Assessment Tests			Terminal Examination
	1	2	3	
Remember	20	20	20	20
Understand	30	20	30	30
Apply	50	60	30	60
Analyse	0	0	20	10
Evaluate	0	0	0	0
Create	0	0	0	0

Course Level Assessment Questions

Course Outcome 1 (CO1):

1. Explain the procedure of Mining with Multiple Minimum Supports
2. Differentiate supervised, unsupervised and partially supervised algorithms.

3. Illustrate the process of mining Sequential Patterns Based on GSP for the following table.

Customer ID	Data Sequence
1	{30} {90}
2	{10, 20} {30} {10, 40, 60, 70}
3	{30, 50, 70, 80}
4	{30} {30, 40, 70, 80} {90}
5	{90}

Course Outcome 2(CO2):

1. Construct a Unified Global Query Interface for railway information system.
2. Consider the following two schemas a, b and integrate the information using matching techniques.
    a. Emp
        i. empNo: int, primary key
        ii. CompName: varchar (60)
        iii. CTname: varchar (15)
        iv. StartDate: date
    b. Employee
        i. EmpID: int, unique
        ii. Company: string
        iii. Contact: string
        iv. Date: date
3. Solve the Roadrunner Algorithm for your own example.

Course Outcome3 (CO3):

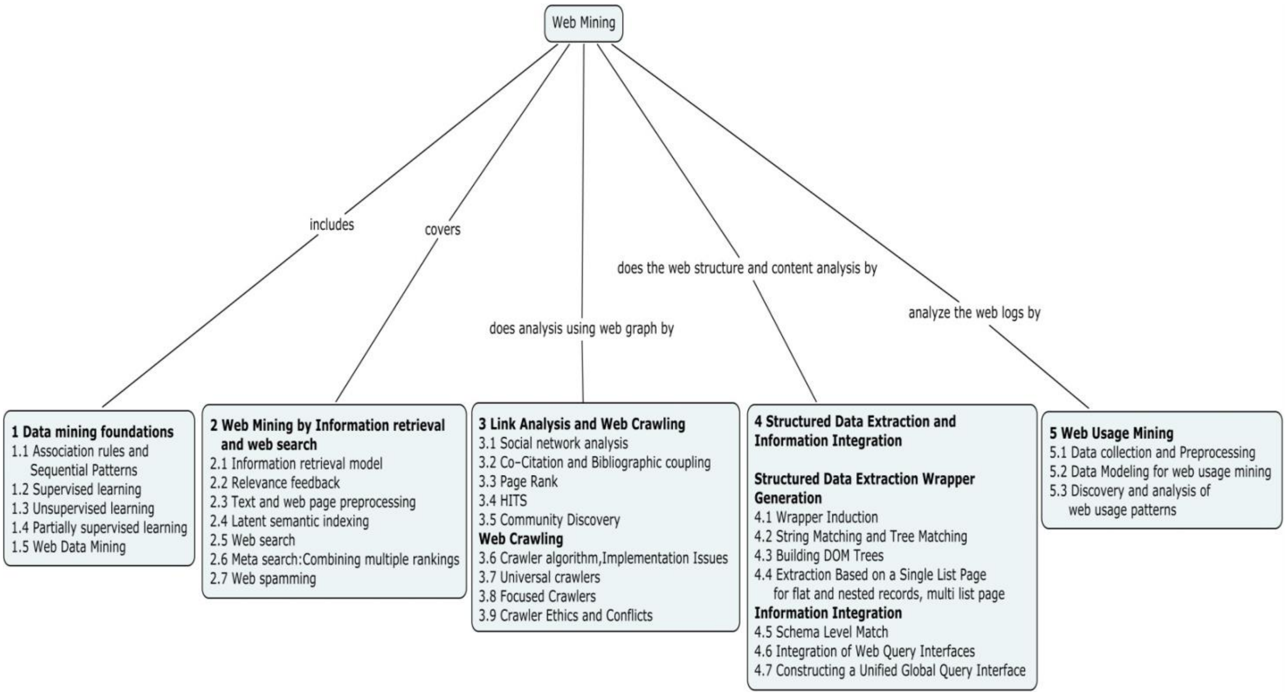
1. Write the Objectives and Actions of Opinion Spamming
2. Solve the following sentences by Identification of Gradable Comparative Sentences
    (a) Sony camera is more expensive than canon camera
    (b) Ram is performing better than ragav.
3. Draw the DOM tree for the following page segment.

Course Outcome 4 (CO4):

1. Illustrate the Steps in data preparation for Web usage mining.
2. Investigate the process of user identification in data collection and pre-processing of web usage.

3. Characterize the Discovery and Analysis of Web Usage Patterns

Concept Map



Syllabus

Data mining foundations: Association rules and Sequential Patterns – supervised learning – unsupervised learning –partially supervised learning-Web Data Mining.

Web Mining by Information retrieval and web search: Information retrieval model – relevance feedback - Text and web page pre-processing – Latent semantic indexing – Web search – Meta search: Combining multiple rankings – web spamming.

Link Analysis and Web Crawling: Social network analysis – Co–Citation and Bibliographic coupling – Page Rank – HITS – Community Discovery. **Web Crawling**- crawler algorithm-Implementation Issues – Universal crawlers – Focused Crawlers – Crawler Ethics and Conflicts**.**

Structured Data Extraction and Information Integration -**Structured Data Extraction Wrapper Generation:** Wrapper Induction- String Matching and Tree Matching -Building DOM Trees -Extraction Based on a Single List Page for flat and nested records, multi list page- **Information Integration**- Schema Level Match-Integration of Web Query Interfaces-Constructing a Unified Global Query Interface -case study on Opinion Mining.

Web Usage Mining: Data collection and Pre-processing – Data Modelling for web usage mining – Discovery and analysis of web usage patterns – case study on Recommender systems and collaborative filtering ,Query Log Mining.

Text Books

1. B. Liu,” Web Data Mining: Exploring Hyperlinks, Contents, and Usage Data “, Springer, Second Edition, 2011.
2. Chakrabarti, S., “Mining the Web”, Morgan Kaufmann publishers (An Imprint of Elsevier) 2005.

Reference Book

1. Anthony Scime, "Web Mining: Applications and Techniques", Yurchack printing inc,2005
2. Alexander Graubner-Müller," Web Mining in Social Media: Use Cases, Business Value, and Algorithmic approach for corporate Intelligence", 2011.

Course Contents and Lecture Schedule

Module No.	Topic	No. of Lectures
1	**Data mining foundations**	
1.1	Association rules and Sequential Patterns	1
1.2	Supervised learning	1
1.3	Unsupervised learning	1
1.4	Partially supervised learning	2
1.5	Web Data Mining	
	Tutorial	2
2	**Web Mining by Information retrieval and web search**	
2.1	Information retrieval model	1
2.2	Relevance feedback	1
2.3	Text and web page pre-processing	1
2.4	Latent semantic indexing	1
2.5	Web search	1
2.6	Meta search: Combining multiple rankings	1
2.7	Web spamming	1
	Tutorial	2
3	**Link Analysis and Web Crawling**	
	Link Analysis	
3.1	Social network analysis	1
3.2	Co –Citation and Bibliographic coupling	1
3.3	Page Rank	1
3.4	HITS	1
3.5	Community Discovery	2
	Tutorial	2
	Web Crawling	
3.6	Crawler algorithm , Implementation Issues	2
3.7	Universal crawlers	1
3.8	Focused Crawlers	1
3.9	Crawler Ethics and Conflicts	1
	Tutorial	1
4	**Structured Data Extraction and Information Integration**	
	Structured Data Extraction Wrapper Generation	
4.1	Wrapper Induction	1
4.2	String Matching and Tree Matching	1
4.3	Building DOM Trees	1
4.4	Extraction Based on a Single List Page for flat and nested records, multi list page	2
	Tutorial	2
	Information Integration	
4.5	Schema Level Match	1

Module No.	Topic	No. of Lectures
4.6	Integration of Web Query Interfaces	1
4.7	Constructing a Unified Global Query Interface	1
	Tutorial	1
	Case study on Opinion Mining	1
5	**Web Usage Mining**	
5.1	Data collection and Pre-processing	1
5.2	Data Modelling for web usage mining	1
5.3	Discovery and analysis of web usage patterns	1
	Tutorial	1
	Case study on Recommender systems and collaborative filtering, Query Log Mining.	1
	Total Lectures	**48**

Course Designers:

1. M.Nirmala Devi mnit@tce.edu
2. S.Karthiga skait@tce.edu

		Category	L	T	P	Credit
14ISPG0	**IT AUDIT AND CONTROL**	PE	3	1	0	4

Preamble

The course aims to provide an understanding of enterprise structure, policies, accountability mechanisms and monitoring practices in place to achieve the requirements of IT governance. Also, knowledge on security architecture (Policies, Standards, Procedures and Controls) and audit services in accordance with IT audit standards to ensure confidentiality, integrity and availability of information assets is provided.

Prerequisite

- Nil

Course Outcomes

On successful completion of the course, the students will be able to

Course Outcomes		**Bloom's Level**
CO1:	Recognize the information security policies, standards and procedures for completeness and alignment with generally accepted practices	Understand
CO2:	Summarize the facts and concepts to be taken into account while conducting periodic reviews of information systems to determine whether they continue to meet the enterprise's objectives.	Understand
CO3:	Solve the IT enterprise related issues in terms of confidentiality, integrity and availability of information.	Apply
CO4:	Compare the effectiveness of the IT governs structure to determine whether IT decisions, directions and performance support the enterprise's strategies and objectives.	Analyze

Mapping with Programme Outcomes

COs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11
CO1.	S	M					M		L	M	
CO2.	S	M			L		M			M	
CO3.	S	S	S		L		M			M	
CO4.	S	S	M						L	M	

S- Strong; M-Medium; L-Low

Assessment Pattern

Bloom's Category	**Continuous Assessment Tests**			**Terminal Examination**
	1	**2**	**3**	
Remember	40	20	20	20
Understand	40	40	40	40
Apply	10	20	20	20
Analyse	0	20	20	20
Evaluate	-	-	-	-
Create	-	-	-	-

Course Level Assessment Questions

Course Outcome 1 (CO1):

1. State the authority of the Office of Internal Audit and the Purpose of Internal Audit report
2. List the responsible persons for internal controls and importance of IT Governance
3. State the Procedure for selecting audits and examine the technique that management uses to addresses the IT issues.
4. Describe the Structure of the information technology function.
5. Identify the information security policies, standards and procedures for completeness

Course Outcome 2 (CO2):

1. Discuss the Disaster Recovery Plan Tests and Drill.
2. Describe how to Provide assurance that the processes for information systems operations, maintenance and support meet the organization’s strategies and objectives
3. Predict the finest way of conducting periodic reviews of information systems.

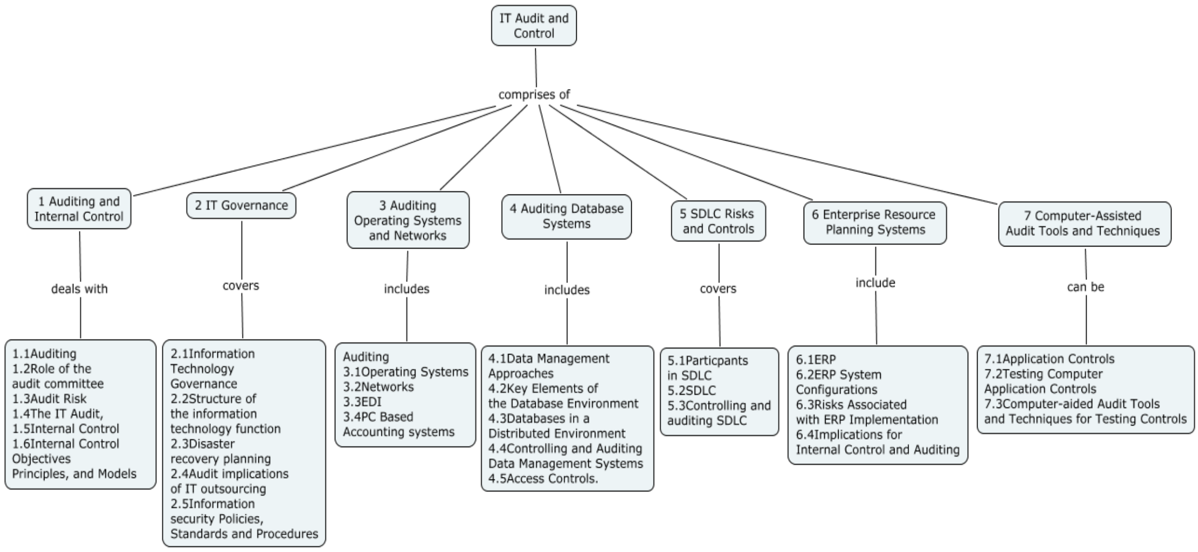
Course Outcome 3 (CO3):

1. Experiment the Triggers of Data Integrity Loss through the following parameters
   a) Vulnerable code-in applications
   b) Unauthorized devices connected to the corporate network
   c) Inadequate or not applied segregation of duties (SoD)
   d) Inability to track the use of privileged passwords, particularly when passwords are shared
2. Report the Attacks on Data Integrity through Web site defacements, Logic bombs and Unauthorized modifications of operating systems etc, by the Following life cycle steps which includes
   a) Entering, creating and/or acquiring data
   b) Processing and/or deriving data
   c) Storing, replicating and distributing data
   d) Archiving and recalling data
   e) Backing up and restoring data
   f) Deleting, removing and destroying data
3. Relate the Standards and Best Practices for Risk Management and Compliance with the Security requirements for data management, information security with COBIT Deliver and Support and manipulate the improvement of the Data Integrity associated with it.

Course Outcome 4 (CO4):

1. Categorize the assurance for the necessary leadership and organization structure and point out the processes that are in place to achieve objectives and to support the organization's strategy.
2. Analyze the IT management and monitoring of controls (e.g., continuous monitoring, QA) for compliance with the organization’s policies, standards and procedure.
3. Identify the actual problem and the incident management practices to determine whether incidents, problems or errors are recorded, analyzed and resolved in a timely manner.

Concept Map



Syllabus

Auditing and Internal Control: Overview of Auditing, Role of the audit committee ,Audit Risk ,The IT Audit, Internal Control, Internal Control Objectives, Principles, and Models.

IT Governance: Information Technology Governance, Structure of the information technology function, disaster recovery planning, audit implications of IT outsourcing.

Auditing Operating Systems and Networks: Auditing Operating Systems, Auditing Networks, Auditing Electronic Data Interchange (EDI),Auditing PC-Based Accounting Systems.

Auditing Database Systems: Data Management Approaches, Key Elements of the Database Environment, Databases in a Distributed Environment, Controlling and Auditing Data Management Systems, Access Controls.

SDLC risks and controls: Participants in Systems Development, the Systems Development Life Cycle, Controlling and Auditing the SDLC.

Enterprise Resource Planning Systems: ERP, ERP System Configurations, Risks Associated with ERP Implementation, Implications for Internal Control and Auditing.

Computer-Assisted Audit Tools and Techniques: Application Controls, Testing Computer Application Controls, Computer-aided Audit Tools and Techniques for Testing Controls.

References

1. James A. Hall, “Information Technology Auditing and Assurance”, South-Western cengage learning ,Third edition, 2011
2. Chris Davis and Mike Schiller, “IT Auditing: Using Controls to protect Information Assets”, Mc-Graw Hill, Second Edition, 2011
3. http://www.isaca.org/knowledge-center/itaf-is-assurance-audit-/IT-Audit-Basics/Pages/IT-Audit-Basics-Articles.aspx
4. http://intosaiitaudit.org/India_GeneralPrinciples.pdf
5. http://opentuition.com/wp-content/blogs.dir/1/files/group-documents/15/1289480671-COMPUTERASSISTEDAUDITTECHNIQUES.pdf

Course Contents and Lecture Schedule

Module No.	Topic	No. of Lectures
1	**Auditing and Internal Control**	
1.1	Overview of Auditing	1
1.2	Role of the audit committee	1
1.3	Audit Risk	2
1.4	The IT Audit	2
1.5	Internal Control	1
1.6	Internal Control Objectives, Principles, and Models.	2
2	**IT Governance**	
2.1	Information Technology Governance	1
2.2	Structure of the information technology function	2
2.3	Disaster recovery planning	1
2.4	Audit implications of IT outsourcing	2
2.5	Information security Policies, Standards and Procedures	3
3	**Auditing Operating Systems and Networks**	
3.1	Auditing Operating Systems	2
3.2	Auditing Networks	2
3.3	Auditing Electronic Data Interchange (EDI)	1
3.4	Auditing PC-Based Accounting Systems	2
4	**Auditing Database Systems**	
4.1	Data Management Approaches	2
4.2	Key Elements of the Database Environment	1
4.3	Databases in a Distributed Environment	1
4.4	Controlling and Auditing Data Management Systems	2
4.5	Access Controls	1
5	**SDLC risks and controls**	
5.1	Participants in Systems Development	1
5.2	The Systems Development Life Cycle	2
5.3	Controlling and Auditing the SDLC	3
6	**Enterprise Resource Planning Systems**	
6.1	ERP	1
6.2	ERP System Configurations	1
6.3	Risks Associated with ERP Implementation	2
6.4	Implications for Internal Control and Auditing	2
7	**Computer-Assisted Audit Tools and Techniques**	
7.1	Application Controls	1
7.2	Testing Computer Application Controls	1
7.3	Computer-aided Audit Tools and Techniques for Testing Controls	2
	Total Lectures	**48**

Course Designers:

1. S.Thiruchadai Pandeeswari eshwarimsp@gmail.com
2. A.Divya divyait@tce.edu
3. C.Santhiya Santhiya.c@gmail.com

14ISPE1	ETHICAL HACKING AND CYBERFORENSICS	Category	L	T	P	Credit
		PE	3	1	0	4

Preamble

This course provides the in-depth knowledge to deploy the tools and techniques needed to protect your network. It also covers cyber forensic investigation, including data recovery and security systems design.

Prerequisite

14IS120 - Cryptography

14IS130 - Network Security

Course Outcomes

On the successful completion of the course, students will be able to

Course Outcomes		Bloom's Level
CO1:	Identify the vulnerabilities in a given network infrastructure	Understand
CO2:	Implement real-world hacking techniques to test system security	Apply
CO3:	Employ complex tools to identify and analyze your company's risks and weaknesses	Apply
CO4:	Apply countermeasures to secure your system against threats	Apply
CO5:	Use the concepts that enable a computer forensic investigator to retrieve evidence for use in criminal investigations.	Understand
CO6:	Apply a number of different computer forensic tools to a given scenario.	Apply

Mapping with Programme Outcomes

COs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11
CO1.	M				L			M	M	M	M
CO2.	M	L	L		M			M	M	M	M
CO3.	M	L	L	L	M	L		M	M	M	M
CO4.	M	L	L		L			M	M	M	M
CO5.	M										
CO6.	M	L	L	L	M	L		M	M	M	M

S- Strong; M-Medium; L-Low

Assessment Pattern

Bloom's Category	Continuous Assessment Tests			Terminal Examination
	1	2	3	
Remember	20	20	20	20
Understand	30	30	30	40
Apply	50	50	50	40
Analyze	0	0	0	0
Evaluate	0	0	0	0
Create	0	0	0	0

Attainment of Course outcomes CO1, CO2, CO3, CO4, CO6 are partially evaluated by Assignments

Course Level Assessment Questions

Course Outcome 1 (CO1):

1. Discuss briefly about the methodologies to collect information from websites, Regional Internet Registries databases and Networks.
2. Describe briefly, how to enumerate the user accounts and devices on a target computer using an application layer protocol that runs on UDP, and which is used to maintain and manage routers, hubs, and switches on an IP network.
3. Outline the different types of techniques used to identify the open ports on a targeted server or host.
4. Compare the various types of attacks in the process of monitoring and capturing all data packets passing through a given network using software (an application) or hardware device.
5. Identify the various threats with countermeasures for E-learning website
6. Explain how Identity thieves use traditional as well as Internet methods to steal identity
7. Explain briefly about compromising Wi-fi Network by gaining unauthorized access to network resources
8. Relate Motives, Goals & Objectives of Information security attacks
9. List the four steps to collect information about the target organization through footprinting
10. Explain the components and need of a security architecture which to bind public keys with corresponding user identities by means of a certificate authority (CA).
11. Infer how the attackers locate network range, determine the operating system, Traceroute to gather information.
12. Discuss briefly about the major threat of social engineering, where the process of stealing someone's identity information used to accomplish the attacker's goals by misusing the information.

Course Outcome 2 (CO2):

1. From the given information, can you identify hosts, ports, and services in a network? Apply in the TCE IT Department Lab network environment and justify your answer.
   i. Establishing the connection between protocols.
   ii. Use fragmented probe packets that reassemble once that reach the targeted host
2. Illustrate how to safeguard the TCE IT Department Lab network from inside and outside attacks by preparing a document or set of documents that describes the security controls, which can be implemented in the lab at a high level.
3. Illustrate with neat sketch, how the attacker perform DOS attacks on a computer or a network by any 4 techniques
4. Use the appropriate techniques to achieve the goals of an attacker:
   i. To collect enough information to gain access
   ii. To create a privileged user account if the user level is obtained
5. Relate the techniques and methodologies used by the attacker to compromise web server
6. Use the process and types of Session Hijacking to perform penetration testing against the services of Banking website
7. Apply the techniques to evade Intrusion Detection System for any Organization network architecture

8. How the attacks use stealth scan to bypass firewall rules and logging mechanism.
9. Name the techniques used by attackers to perform enumeration.
10. Identify the techniques or the type of attacks the attacker adopts to hack a system or a network
11. Dramatize the various methods to detect the memory corruption issues which would allow an attacker to abuse the way the Steam client handles browser requests
12. Apply the port scanning techniques to identify running services on a host with the intent of compromising it.
13. Examine how user accounts and devices are enumerated from the target system
14. Outline the role of the penetration tester to perform pen testing for Trojans and Backdoors.

Course Outcome 3 (CO3):

1. Sequence and prepare the report for tools as an ethical hacker to determine organization's publicly available information on the Internet such as network architecture, operating systems, applications, and users.
2. Sequence and prepare the report for tools as an ethical hacker to identify system attack points and perform password attacks to gain unauthorized access to information system resources.
3. Perform Penetration testing and defend against buffer overflow attacks for a college website
4. Sequence and prepare the report for tools as an ethical hacker to determine organization's publicly available information on the Internet such as network architecture, operating systems, applications, and users

Course Outcome 4 (CO4):

1. Demonstrate how the procedures for changing attacker IP address so that attacker appears to be someone else can be detected and provide any 2 appropriate countermeasures.
2. Prepare and sequence the actions of Physical security check list for the Cyberforensics lab of TCE-IT Department
3. Apply the wireless encryption standards (WEP, WAP and WAP2) for protecting the TCE-Wifi networks from attackers, who collects sensitive information by breaching the Radio frequency traffic.
4. "At present, most businesses use email as the major source of communication as it is simple and easy to communicate or share information. These emails may contain sensitive information about their projects, updates, etc. If this information falls in to the wrong hands, then the organizations may face huge losses." - Determine security mechanisms to avoid the risk faced by the business organizations

Course Outcome 5 (CO5):

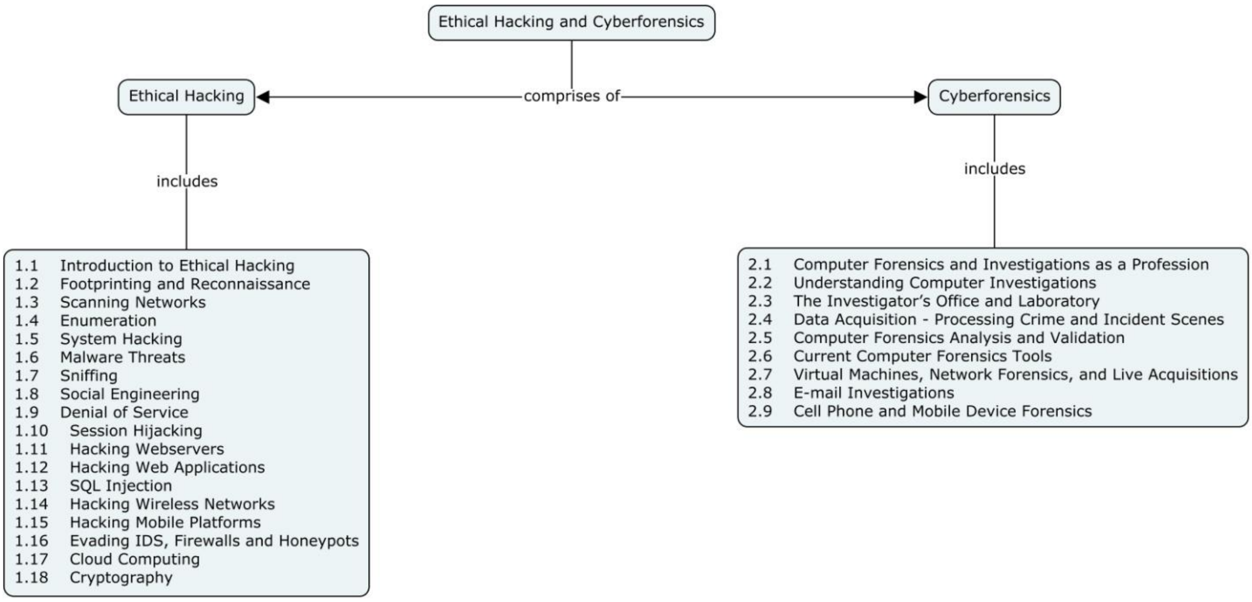
1. In computer forensics,
   i. Distinguish between Identity theft and Identity Fraud.
   ii. Outline the features and problems of Traditional computer crime.
2. Illustrate the different types of computer forensics with traditional systematic approach of computer investigations
3. Demonstrate the essential and methods to analyze and validate the digital evidence.
4. Infer the ways to determine the best data acquisition method for Cyber Investigation.
5. Dramatize the different types of computer forensics with traditional systematic approach of computer investigations for cyber attacks in web server

6. Relate the common data hiding techniques to analyze and validate the viruses or trojans in a desktop computer

Course Outcome 6 (CO6):

1. Summarize the needs, availability, considerations, methods for validating and testing the computer forensic tools
2. Identify the various data acquisition methods with forensic tools to transfer the digital evidence for forensic analysis
3. Relate the process of investigation in E-mail and Mobile device Forensics
4. Outline the five major tasks performed by Computer forensics Tools.
5. Articulate the procedures to acquire logs or screenshots of attackers tasks from cell phone and mobile devices
6. As a Cyber forensic investigator, examine the roles, tasks and tools for investigating Lottery Winner - forgery email

Concept Map



Syllabus

Ethical Hacking: Introduction to Ethical Hacking - Footprinting and Reconnaissance - Scanning Networks - Enumeration - System Hacking - Malware Threats - Sniffing - Social Engineering - Denial of Service - Session Hijacking - Hacking Webservers - Hacking Web Applications - SQL Injection - Hacking Wireless Networks - Hacking Mobile Platforms - Evading_IDS, Firewalls and Honeypots - Cloud Computing – Cryptography

Cyber Forensics: Computer Forensics and Investigations as a Profession - Understanding Computer Investigations - The Investigator's Office and Laboratory - Data Acquisition - Processing Crime and Incident Scenes - Computer Forensics Analysis and Validation - Current Computer Forensics Tools - Virtual Machines, Network Forensics, and Live Acquisitions - E-mail Investigations - Cell Phone and Mobile Device Forensics

Text Books

1. CEH official Certfied Ethical Hacking Review Guide, Wiley India Edition, 2015.
2. Bill Nelson, Amelia Phillips, Christopher Steuart, "Guide to Computer Forensics and Investigations", Delmar Cengage Learning, 2015.

References

1. Ankit Fadia " Ethical Hacking" second edition Macmillan India Ltd, 2006
2. Kenneth C.Brancik "Insider Computer Fraud" Auerbach Publications Taylor & Francis Group–2008.
3. John R. Vacca, "Computer Forensics: Computer Crime Scene Investigation", 2nd Edition, CharlesRiver Media, 2008.

Course Contents and Lecture Schedule

Module No.	Topic	No. of Lectures
1	**Ethical Hacking**	
1.1	Introduction to Ethical Hacking	1
1.2	Footprinting and Reconnaissance	2
1.3	Scanning Networks	2
1.4	Enumeration	1
1.5	System Hacking	2
1.6	Malware Threats	2
1.7	Sniffing	1
1.8	Social Engineering	1
1.9	Denial of Service	1
1.10	Session Hijacking	2
1.11	Hacking Webservers	3
1.12	Hacking Web Applications	3
1.13	SQL Injection	2
1.14	Hacking Wireless Networks	2
1.15	Hacking Mobile Platforms	2
1.16	Evading IDS, Firewalls and Honeypots	3
1.17	Cloud Computing	1
1.18	Cryptography	1
2	**Cyber Forensics**	
2.1	Computer Forensics and Investigations as a Profession	1
2.2	Understanding Computer Investigations	2
2.3	The Investigator's Office and Laboratory	1
2.4	Data Acquisition - Processing Crime and Incident Scenes	3
2.5	Computer Forensics Analysis and Validation	2
2.6	Current Computer Forensics Tools	1
2.7	Virtual Machines, Network Forensics, and Live Acquisitions	2
2.8	E-mail Investigations	2
2.9	Cell Phone and Mobile Device Forensics	2
Total Lectures		**48**

Course Designers:

1.	R. Leena Sri	rlsit@tce.edu
2.	M. Thangavel	mtit@tce.edu
3.	S.Karthiga	skait@tce.edu

		Category	L	T	P	Credit
14ISPF1	**CLOUD AND SECURITY**	PE	3	1	0	4

Preamble

As organizations transition to cloud computing technology, security issues are a vital concern. In order to protect sensitive data and maintain regulatory compliance, the course must address the unique cyber security challenges faced when moving to a cloud environment. This course provides an experience of identifying and resolving the security issues specific to public and private clouds.

Prerequisite

- 14IS170: Cryptography and Network Security Lab

Course Outcomes

On the successful completion of the course, students will be able to

Course Outcomes		**Bloom's Level**
CO1:	Understand the systems, protocols and mechanisms to support cloud computing architectural framework.	Understand
CO2:	Outline the cloud computing security challenges and security controls recommendation.	Understand
CO3:	Compare modern security concepts as they are applied to cloud computing.	Analyze
CO4:	Examine the security of virtual systems and analyze the security issues related to multi-tenancy.	Analyze
CO5:	Demonstrate compliance and trust issues that arise from cloud computing.	Apply

Mapping with Programme Outcomes

COs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11
CO1.	L										
CO2.	L										
CO3.	S	S	S	M	M				M	M	
CO4.	S	S	S	M	M	L	L	L	M	M	L
CO5.	M	M	M						L	L	

S- Strong; M-Medium; L-Low

Assessment Pattern

Bloom's Category	Continuous Assessment Tests			Terminal Examination
	1	2	3	
Remember	20	0	0	20
Understand	30	20	20	30

Apply	30	40	40	40
Analyse	20	40	40	10
Evaluate	0	0	0	0
Create	0	0	0	0

Attainment of Course outcome 3, 4 and 5 is partially evaluated by Assignments.

Course Level Assessment Questions

Course Outcome 1 (CO1):

1. How does cloud computing provides on-demand functionality?
2. What resources are provided by infrastructure as a service?
3. What does software as a service provide?
4. What essential things a user should know before going for cloud computing platform?

Course Outcome 2 (CO2):

1. What are the security aspects provided with cloud?
2. What are the security laws which take care of the data in the cloud?
3. How to secure your data for transport in cloud?
4. Give an overview of Open Stack Services

Course Outcome 3 (CO3):

1. How does encryption provide cloud security for the data's stored in cloud.
2. Discuss about the various cloud security apps.
3. Does authentication and authorization are needed for cloud security.

Course Outcome 4 (CO4):

1. Discuss in detail virtualization system security issues.
2. Analyze the various cloud computing tools to improve security through automation.
3. What are optimizing strategies used in cloud?

Course Outcome 5 (CO5):

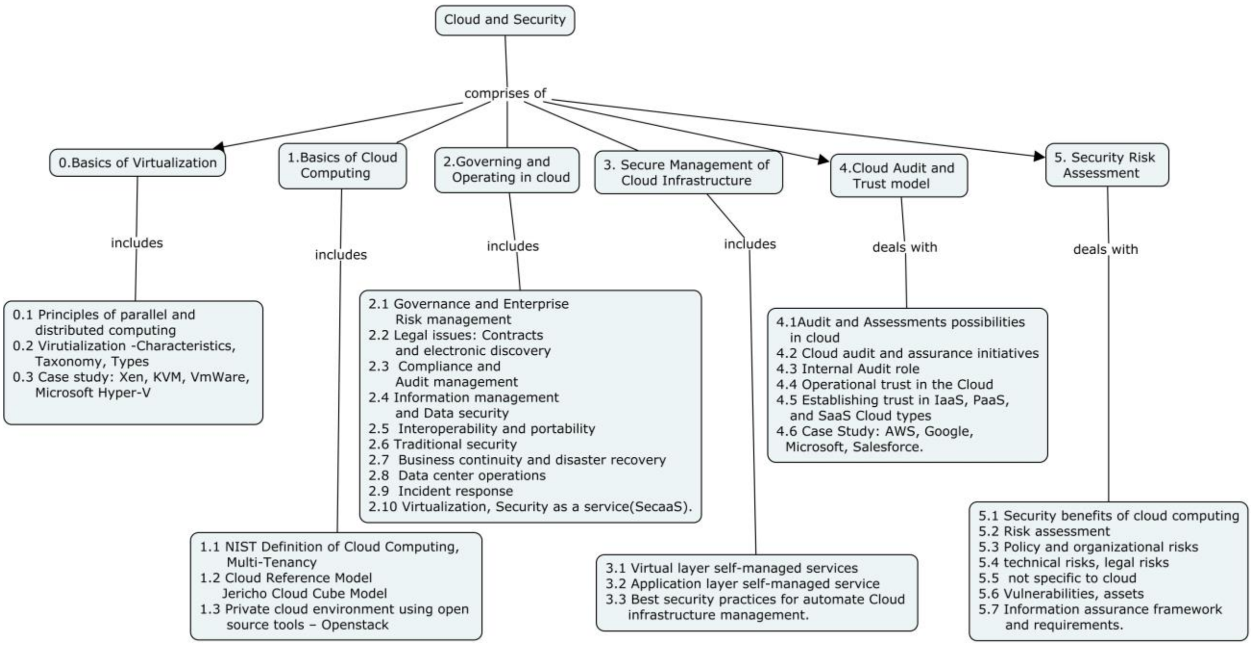
1. Assume that a company ABC wants to offer services such as starting a policy and payment of policy on a service oriented architecture over the cloud. Explain the implementation details of this scenario.
2. Consider a Ubuntu virtual machine installed over a windows machine. Explain the SNAT and DNAT configuration that needs to be applied to enable the Ubuntu virtual machine communication with the external network and the external network communication with the Ubuntu virtual machine.
3. Explain IBM application services for cloud security.

Some of the Assignments topics are: (but not limited to)

1. Providing Cyber Security lab as a Service
2. Service deployment and usage over cloud
3. Managing cloud computing resources
4. Demonstrate existing cloud characteristics and service models

5. Performance evaluation of Services over cloud

Concept Map



Syllabus

Basics of Virtualization - Principles of parallel and distributed computing, Virtualization-Characteristics, Taxonomy, Types, Case study: Xen, KVM, VmWare, Microsoft Hyper-V.

Basics of Cloud Computing - NIST Definition of Cloud Computing, Multi-Tenancy, Cloud Reference Model, Jericho Cloud Cube Model, Private cloud environment using open source tools – Openstack, OpenNebula

Governing and operating in cloud: Governance and Enterprise Risk management, Legal issues: Contracts and electronic discovery, Compilance and Audit management, Information management and Data security, Interoperability and portability. Traditional security, Business continuity and disaster recovery, Data center operations, Incident response, Virtualization security, Security as a service(SecaaS)

Secure Management of Cloud Infrastructure: Virtual layer self-managed services, application layer self-managed service, best security practices for automate Cloud infrastructure management.

Cloud Audit and Trust model: Audit and Assessments possibilities in cloud, Cloud audit and assurance initiatives, Internal Audit role. Operational trust in the Cloud, Establishing trust in IaaS, PaaS, and SaaS Cloud types, Case Study: AWS, Google, Microsoft, Salesforce,

Security Risk Assessment: Security benefits of cloud computing, Risk assessment, Policy and organizational risks, technical risks, legal risks, risks not specific to cloud, vulnerabilities, assets, Information assurance framework and requirements.

Text Book

1. Rajkumar Buyya, Christian Vecchiola, S.Thamarai Selvi, “Mastering cloud computing”, Morgan Kaufman, 2013.
2. Cloud Security Alliance whitepaper, “Security Guidance for Critical Areas of Focus in Cloud Computing” 3rd version, 2011

Siani Pearson, George Yee "Privacy and Security for Cloud Computing" Computer Communications and Networks, Springer, 2013

References

1. The European Union Agency for Network and Information Security, “Cloud computing security risk assessment”, https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment/at_download/fullReport, 2009.
2. Cloud Security Alliance, “Providing greater clarity in Security as a Service” https://cloudsecurityalliance.org/group/security-as-a-service/, 2013.
3. The National IT and Telecom Agency, “Cloud audit and assurance initiatives” www.digst.dk/~/media/Files/.../**Cloud-Audit-and-Assurance**-EN_cagr.pdf, 2011
4. Toby Velte, Anthony Velte, Robert Elsenpeter, “Cloud Computing, A Practical Approach” McGraw-Hill Osborne Media; 1 edition [ISBN: 0071626948], 2009.

Course Contents and Lecture Schedule

Module No.	Topic	No. of Lectures
0	**Basics of Virtualization**	
0.1.	Principles of parallel and distributed computing,	2
0.2	Virtualization- Characteristics, Taxonomy, Types	2
0.3	Case study: Xen, KVM, VmWare, Microsoft Hyper-V	2
1	**Basics of Cloud Computing**	
1.1	NIST Definition of Cloud Computing, Multi-Tenancy	2
1.2	Cloud Reference Model, Jericho Cloud Cube Model	2
1.3	Private cloud environment using open source tools – Openstack,	2
2	**Governing and Operating in cloud**	
2.1	Governance and Enterprise Risk management	2
2.2	Legal issues: Contracts and electronic discovery	2

2.3	Compliance and Audit management	2
2.4	Information management and Data security	2
2.5	Interoperability and portability	2
2.6	Traditional security	2
2.7	Business continuity and disaster recovery	1
2.8	Data center operations	1
2.9	Incident response	1
2.10	Virtualization, Security as a service(SecaaS).	1
3	**Secure Management of Cloud Infrastructure**	
3.1	Virtual layer self-managed services	2
3.2	application layer self-managed service	2
3.3	best security practices for automate Cloud infrastructure	1
4	**Cloud Audit and Trust model**	
4.1	Audit and Assessments possibilities in cloud	1
4.2	Cloud audit and assurance initiatives	2
4.3	Internal Audit role	1
4.4	Operational trust in the Cloud	1
4.5	Establishing trust in IaaS, PaaS, and SaaS Cloud types	1
4.6	Case Study: AWS, Google, Microsoft, Salesforce.	1
5	**Security Risk Assessment**	
5.1	Security benefits of cloud computing	1
5.2	Risk assessment	1
5.3	Policy and organizational risks	1
5.4	technical risks, legal risks	1
5.5	risks not specific to cloud	1
5.6	Vulnerabilities, assets	1
5.7	Information assurance framework and requirements.	2
	Total Lectures	**48**

Course Designers:

1. C. Jeyamala jeyamala@tce.edu
2. M. Thangavel mtit@tce.edu
3. S. Raja Lavanya lavanyachakkaravarthy@gmail.com

OUTCOME BASED EDUCATION

CURRICULUM AND DETAILED SYLLABI

FOR

M.E COMPUTER SCIENCE AND INFORMATION SECURITY DEGREE PROGRAMME

PROGRAMME ELECTIVES

FOR THE STUDENTS ADMITTED IN THE

ACADEMIC YEAR 2014-15 ONWARDS

THIAGARAJAR COLLEGE OF ENGINEERING

(A Government Aided ISO 9001:2008 certified Autonomous Institution affiliated to Anna University)

MADURAI – 625 015, TAMILNADU

Phone: 0452 – 2482240, 41
Fax: 0452 2483427
Web: www.tce.edu

14ISPH0	**INFORMATION RETRIEVAL TECHNIQUES**	Category	L	T	P	Credit
		PE	3	1	0	4

Preamble

The course focuses on the representation, storage, organization of, and access to information items using various IR algorithms and techniques. The course emphasizes the building of information retrieval systems for documents so as to retrieve relevant or useful information from them.

Prerequisite

- **Nil**

Course Outcomes

On the successful completion of the course, students will be able to

Course Outcomes		**Bloom's Level**
CO1:	Use information retrieval modelling techniques for Corpus documents	Apply
CO2:	Apply query processing techniques to locate relevant information from the large collection of data	Apply
CO3:	Apply machine learning techniques for information retrieval from textual data	Apply
CO4:	Evaluate different information retrieval systems for web search tasks	Analyze
CO5:	Develop simple information retrieval system for applications like personalization and recommender systems, search engines, etc	Analyze

Mapping with Programme Outcomes

COs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11
CO1.	**S**										
CO2.	**S**	**M**									
CO3.	**S**	**S**	**S**	**M**							
CO4.	**S**	**S**	**S**	**M**	**S**			**S**	**S**	**S**	
CO5.	**S**	**S**	**S**	**M**	**S**			**S**	**S**	**S**	**L**

S- Strong; M-Medium; L-Low

Assessment Pattern

Bloom's Category	**Continuous Assessment Tests**			**Terminal Examination**
	1	**2**	**3**	
Remember	20	20	10	10
Understand	30	20	10	30
Apply	50	40	40	50
Analyze	0	20	30	10
Evaluate	0	0	10	0
Create	0	0	0	0

Course Level Assessment Questions

Course Outcome 1 (CO1)

1. Find the inverted index that would be built for the given set of documents.

2. Draw the term-document incidence matrix for the given document collection.
3. Consider the table of term frequencies for the set of documents. Compute tf-idf weights for the given terms.
4. Compute Euclidean normalized document vectors for each of the documents.
5. An IR system returns 8 relevant documents and 10 non relevant documents from the set of 20 documents. Compute precision, recall and F-measure values.

Course Outcome 2 (CO2)

1. Explain how the Boolean query x and not y be handled.
2. Explain the principled approaches for assigning weights to query terms.
3. Suppose the query tem is not in the document collection, how would one adapt hte vector space representation to handle this situation?
4. State three reasons why relevance feedback has been little used in web search.
5. Positive feedback is likely to be more useful than negative feedback. Justify.

Course Outcome 3 (CO3)

1. Describe the differences between vector space and probabilistic model for the information retrieval of text documents.
2. Describe indexing in information retrieval.
3. Classify the given set of documents using Naive Bayes theorem.
4. Describe document clustering for text data.

Course Outcome 4 (CO4)

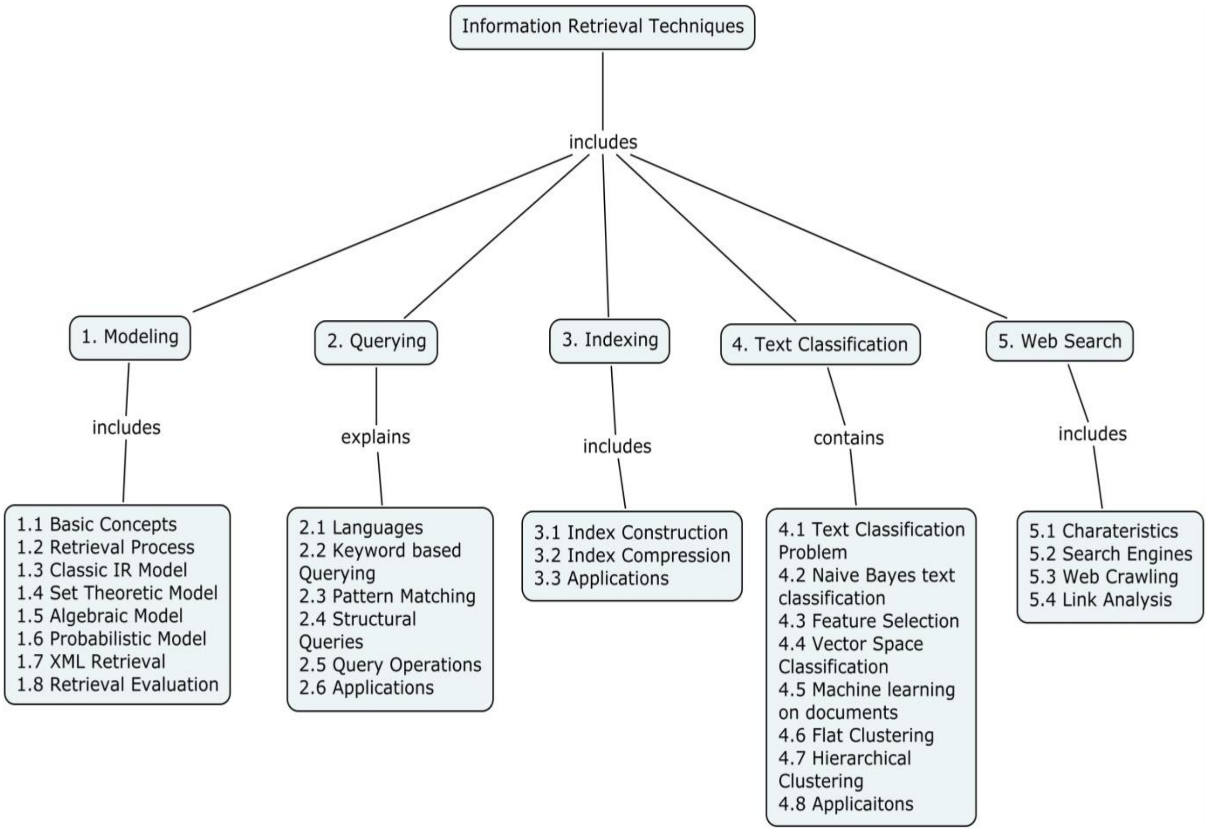
1. Analyze the reasons why relevance feedback has been little used in web search.
2. Write down the transition probability matrix of given figure.
3. A user uses links to traverse forward and back button to move backward. Justify whether Markov chain can be used as a model in this case.
4. Show that the page rank of every page is at least α/N.

Course Outcome 5 (CO5)

Development of simple IR system for a given domain such as,

1. Web media
2. Social network
3. Management structure
4. Document retrieval

Concept Map



Syllabus

Modeling Basic Concepts – Retrieval Process – Classic Information Retrieval Models – Boolean Model – Vector Model – Probabilistic Model – Set Theoretic Model – Fuzzy Set Model – Extended Boolean Model - Algebraic Model – Vector Space Model – Latent semantic indexing model – Alternative Probabilistic Model – Bayesian Networks – XML Retrieval - Retrieval Evaluation

Querying Languages – Key Word based Querying – Pattern Matching – Structural Queries – Query Operations – User Relevance Feedback – Local and Global Analysis - Applications

Indexing Index Construction – Index Compression - Applications

Text Classification Text classification problem – Naïve Bayes text classification – Feature Selection – Vector Space Classification – Machine learning on documents – Flat Clustering – Hierarchical Clustering - Applications

Web Search Characteristics – Search Engines – Web Crawling – Link Analysis - Applications

References

1. Ricardo Baeza-Yates, Berthier Ribeiro-Neto, “Modern Information Retrieval”, Pearson Education, Second Edition,2011.
2. Christopher D. Manning, Prabhakar Raghavan, and Hinrich Schütze, “An Introduction to Information Retrieval”, Cambridge University Press, Cambridge, England, 2007.

3. http://www.cs.utexas.edu/users/mooney/ir-course
4. http://www.ischool.washington.edu/efthimis/courses/lis544
5. http://www.informationretrieval.

Course Contents and Lecture Schedule

S. No	Topic	No. of Lectures
1	**Modeling**	
1.1	Basic Concepts	1
1.2	Retrieval Process	1
1.3	Classic Information Retrieval Models	
1.3.1	Boolean Model	2
1.3.2	Vector Model	2
1.3.3	Probabilistic Model	2
1.4	Set Theoretic Models	
1.4.1	Fuzzy Set Model	1
1.4.2	Extended Boolean Model	1
1.5	Algebraic Models	
1.5.1	Vector Space Model	2
1.5.2	Latent Semantic Indexing Model	2
1.6	Alternative Probabilistic Models	
1.6.1	Bayesian Networks	1
1.7	XML Retrieval	1
1.8	Retrieval Evaluation	1
2	**Querying**	
2.1	Languages	1
2.2	Keyword based querying	1
2.3	Pattern Matching	1
2.4	Structural Queries	1
2.5	Query Operations	
2.5.1	User Relevance Feedback	2
2.5.2	Local and Global Analysis	2
2.6	Applications	1
3	**Indexing**	
3.1	Index Construction	2
3.2	Index Compression	2
3.3	Applications	1
4	**Text Classification**	
4.1	Text Classification Problems	1
4.2	Naive Bayes text classification	2
4.3	Feature Selection	1
4.4	Vector Space Classification	1
4.5	Machine Learning on documents	2
4.6	Flat Clustering	1
4.7	Hierarchical Clustering	1
4.8	Applications	1
5	**Web Search**	
5.1	Characteristics	1
5.2	Search Engines	1
5.3	Web Crawling	2

5.4	Link Analysis	2
5.5	Applications	
	Total Lectures	**36**

Course Designers:

1. Ms.A.M.Abirami abiramiam@tce.edu
2. Ms.K.V.Uma kvuit@tce.edu

14ISPI0	**DISTRIBUTED OPERATING SYSTEMS AND SECURITY**	Category	L	T	P	Credit
		PE	3	1	0	4

Preamble

This course provides an in-depth examination of the principles of distributed systems in general, and distributed operating systems in particular. Covered topics include processes and threads, concurrent programming, distributed inter process communication, distributed process scheduling, virtualization, distributed file systems, security in distributed systems, distributed middleware and applications such as the web and peer-to-peer systems.

Prerequisite

- Nil

Course Outcomes

On the successful completion of the course, students will be able to

Course Outcomes		**Bloom's Level**
CO1:	Identify core concepts of distributed systems	Understand
CO2:	Develop practical skills of implementation of distributed algorithms in software	Apply
CO3:	Manipulate theoretical models used to design distributed systems.	Apply
CO4:	Examine state –of-art distributed systems, such as Google File System	Analyze
CO5:	Analyze the security issues and mechanism to secure the system	Analyze

Mapping with Programme Outcomes

COs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1.	M											
CO2.	S	M	L		S		M	L	M			L
CO3.	S	M	L		S		M	L	M			L
CO4.	S	S	M	L		L	L	L	M	M	L	L
CO5.	S	S	M	L		L	L	L		M	L	L

S- Strong; M-Medium; L-Low

Assessment Pattern

Bloom's Category	**Continuous Assessment Tests**			**Terminal Examination**
	1	**2**	**3**	
Remember	20	20	20	20
Understand	50	20	20	40
Apply	30	50	50	40
Analyze	0	10	10	0
Evaluate	0	0	0	0
Create	0	0	0	0

Attainment of Course outcome 2, 3 and 4 is partially evaluated through Assignments.

Course Level Assessment Questions

Course Outcome 1 (CO1):

1. List out the goals in distributed systems
2. Identify the kind of consistency used to implement an electronic stock market? Explain your answer.
3. Explain the Identification of the concurrent events using logical clock and steps for implementing logical clock with an example

Course Outcome 2 (CO2):

1. Devise a distributed algorithm for computing a spanning tree of a connected undirected graph in which no root is designated. You can assume that the nodes have unique names.
2. Devise an algorithm which synchronize 'n' no. of customers accessing the banking databases and recovery procedure if there occurs sudden crash in application server
3. Design a distributed application which consist of a Agent program that program travels in the network and performs a given task on the targeted node. You may assign any task to the agent for example to carry out a file reading/processing at the remote machine and so on.

Course Outcome 3 (CO3):

1. A user arrives at a railway station that she has never visited before, carrying a PDA that is capable of wireless networking. Suggest how the user could be provided with information about the local services and amenities at that station, without entering the station's name or attributes. What technical challenges must be overcome?
2. Compare reading a .le using a single-threaded idle server and a multithreaded server. It takes 15 msec to get a request for work, dispatch it, and do the rest of the necessary processing, assuming that the data needed are in a cache in main memory. If a disk operation is needed, as is the case one-third of the time, an additional 75 msec is required, during which time the thread sleeps. How many requests/sec can the server handle if it is single threaded? If it is multithreaded?
3. Sketch the design of a multithreaded server that supports multiple protocols using sockets as its transport-level interface to the underlying operating system.

Course Outcome 4 (CO4):

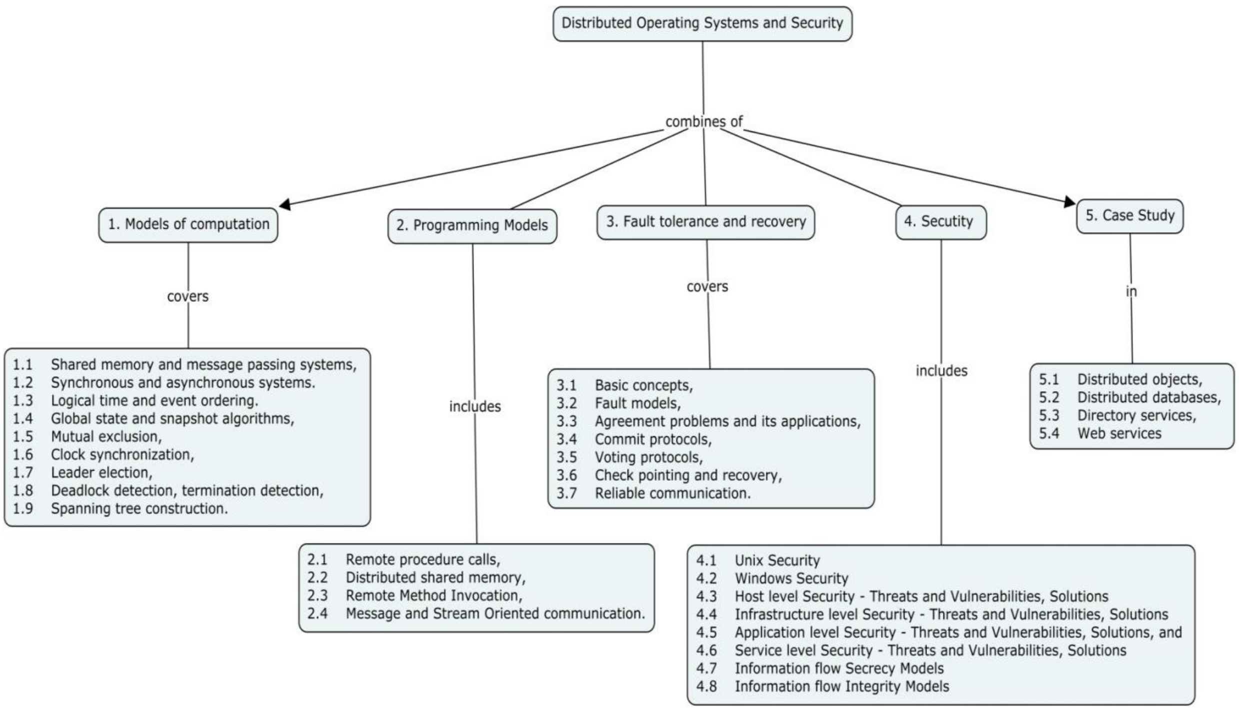
1. Consider a chain of processes *P*1, *P*2, ..., *Pn* implementing a multitiered client-server architecture. Process *Pi* is client of process *Pi*+1, and *Pi* will return a reply to *Pi*-1 only after receiving a reply from *Pi*+1. What are the main problems with this organization when taking a look at the request-reply performance at process *P*1
2. Apply how replication in Domain Naming service takes place and how it actually works so well in client centric consistency
3. Select a proper approach which makes the decision and never gets blocked even after the coordinator crashes in two-phase commit

Course Outcome 5 (CO5):

1. Discuss briefly about the levels of security provide across distributed in UNIX and Windows operating systems.

2. Compare and contrast the different levels of security essential in distributed operating systems.
3. Examine the Threats and vulnerabilities available in Distributed Host, Application and Service.

Concept Map



Syllabus

Models of computation: Shared memory and message passing systems, synchronous and asynchronous systems. Logical time and event ordering. Global state and snapshot algorithms, mutual exclusion, clock synchronization, leader election, deadlock detection, termination detection, spanning tree construction.
Programming models: Remote procedure calls, distributed shared memory, Remote Method Invocation, Message and Stream Oriented communication.
Fault tolerance and recovery: Basic concepts, fault models, agreement problems and its applications, commit protocols, voting protocols, check pointing and recovery, reliable communication.
Security: Unix & Windows Security – Protection system, Authorization, Security analysis, Vulnerabilities. Host level, Infrastructure level, Application level, and Service level security - Threats and Vulnerabilities, Solutions. Information flow Secrecy Models – Denning's Lattice Model, Bell LaPadula Model. Information flow Integrity Models – Biba Integrity model, Low-Water Mark Integrity, Clark-Wilson Integrity.
Case Study: distributed objects, distributed databases, directory services, web services.

Text Book

1. N. Lynch, Distributed Algorithms, Elsevier India Private Limited, (2009)
2. Hagit Attiya, Jennifer Welch, Distributed Computing: Fundamentals, Simulations and Advanced Topics, Wiley, (2006)
3. Trent Jaeger, "Operating System Security", Morgan & Claypool publishers, (2008).

4. Abhijit Belapurkar, Anirban Chakrabarti, Harigopal Ponnapalli, Niranjan Varadarajan, Srinivas Padmanabhuni, Srikanth Sundarrajan, “Distributed Systems Security: Issues, Processes and Solutions”, Wiley, (2009).

References

1. S.Ghosh, Distributed Systems: An Algorithmic Approach, Chapman & Hall, (2006)
2. A. Kshemkalyani, M. Singhal, Distributed Computing: Principles, Algorithms, and Systems, Cambridge University Press, (2008)
3. Gerard Tel, Introduction to Distributed Algorithms, 2nd edition, Cambridge University Press, (2004)
4. Technical papers from major distributed systems journals and conferences

Course Contents and Lecture Schedule

S.No.	Topic	No. of Lectures
1	**Models of computation**	
1.1	Shared memory and message passing systems,	**1**
1.2	Synchronous and asynchronous systems.	**1**
1.3	Logical time and event ordering.	
1.4	Global state and snapshot algorithms,	**1**
1.5	Mutual exclusion,	**1**
1.6	Clock synchronization,	
1.7	Leader election,	**1**
1.8	Deadlock detection, termination detection,	**1**
1.9	Spanning tree construction.	**1**
2	**Programming models**	
2.1	Remote procedure calls,	1
2.2	Distributed shared memory,	1
2.3	Remote Method Invocation,	
2.4	Message and Stream Oriented communication.	1
3	**Fault tolerance and recovery**	
3.1	Basic concepts,	1
3.2	Fault models,	1
3.3	Agreement problems and its applications,	1
3.4	Commit protocols,	1
3.5	Voting protocols,	1
3.6	Check pointing and recovery,	1
3.7	Reliable communication.	1
4	**Security**	
4.1	Unix Security	1
4.1.1	Protection system,	
4.1.2	Authorization,	
4.1.3	Security analysis,	1
4.1.4	Vulnerabilities.	
4.2	Windows Security	1
4.2.1	Protection system,	

4.2.2	Authorization,	
4.2.3	Security analysis,	1
4.2.4	Vulnerabilities.	
4.3	Host level Security - Threats and Vulnerabilities, Solutions	2
4.4	Infrastructure level Security - Threats and Vulnerabilities, Solutions	2
4.5	Application level Security - Threats and Vulnerabilities, Solutions, and	2
4.6	Service level Security - Threats and Vulnerabilities, Solutions	2
4.7	Information flow Secrecy Models	1
4.7.1	Denning's Lattice Model,	
4.7.2	Bell LaPadula Model.	
4.8	Information flow Integrity Models	2
4.8.1	Biba Integrity model,	
4.8.2	Low-Water Mark Integrity,	
4.8.3	Clark-Wilson Integrity	
5	**Case Study**	
5.1	Distributed objects,	1
5.2	Distributed databases,	1
5.3	Directory services,	1
5.4	Web services	1
	Total Lectures	**36**

Course Designers:

1. Ms.R.Leena Sri rlsit@tce.edu
2. Mr.M.Thangavel mtit@tce.edu

		Category	L	T	P	Credit
14ISPJ0	**NETWORK PENETRATION TESTING**	PE	3	1	0	4

Preamble

A penetration test is a real world security test that determines how well the security defences are protecting your IT assets. The network penetration tester goal is to gain unauthorized access to IT assets and subsequently access to confidential data before the bad guys do. The network penetration testing approach is often driven by the objectives of the organization as well as a clear definition of which security defences are to be tested. Network penetration testing helps address the concerns about the actual impact an attack could have on the organization.

Prerequisite

- 14IS120 - Cryptography
- 14IS130 - Network Security
- 14IS210 - System Security

Course Outcomes

On the successful completion of the course, students will be able to

Course Outcomes		**Bloom's Level**
CO1:	Defend against the most common attacks to networks.	Apply
CO2:	Estimate the needs and constraints of a given concern's scenario to determine what type of firewall solution, Intrusion detection and prevention system is appropriate.	Evaluate
CO3:	Use point-to-point tunnelling protocol (PPTP), layer 2 tunnelling protocol (L2TP) as an encryption tool and add security with privacy to a communication using IPSec for VPNs.	Apply
CO4:	Configure Windows and Linux systems for secure operations.	Apply
CO5:	Formulate an appropriate strategy to defend against virus attacks, Trojan Horses, Spyware, and Adware	Analyze
CO6:	Assess the system and wireless network security through security policies, physical security, business continuity and security standards.	Evaluate

Mapping with Programme Outcomes

COs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11
CO1.	**M**	**L**	**L**		**M**	**L**		**L**	**M**	**L**	**L**
CO2.	**M**	**L**	**L**	**L**	**M**	**L**		**L**	**M**		
CO3.	**M**	**L**	**L**		**M**				**M**		
CO4.	**M**	**L**	**L**		**M**				**M**		**L**
CO5.	**M**	**L**	**L**		**M**	**L**		**L**	**M**	**L**	**L**
CO6.	**M**	**L**	**L**	**L**	**L**				**M**		

S- Strong; M-Medium; L-Low

Assessment Pattern

Bloom's Category	Continuous Assessment Tests			Terminal Examination
	1	2	3	
Remember	20	0	0	20
Understand	50	20	40	40
Apply	30	40	40	40
Analyse	0	20	10	0
Evaluate	0	20	10	0
Create	0	0	0	0

Attainment of Course outcomes CO2, CO5, CO6 are partially evaluated by Assignments

Course Level Assessment Questions

Course Outcome 1 (CO1):

1. Demonstrate the basic DoS attack by Setting up a machine with a Web server, Use other machines in the lab to begin pinging the target machine, Continue this until the target is no longer able to respond to legitimate requests, and Note the number of total packets per second required to successfully execute a DoS attack.
2. Considering how buffer overflow vulnerabilities arise, explain why you think they are present and provide recommendations to prevent or reduce the number of such flaws.
3. Using the Internet, journals, books, or other resources, find one incident of a Trojan horse attack in the past nine months. How was this Trojan horse delivered? What damage did it cause? Describe the Trojan horse attack, including:
   - Any specific targets
   - Whether the perpetrators of the attack have been caught and/or prosecuted
   - What types of security warnings were issued about the attack as well as measures prescribed to defend against it.

Course Outcome 2 (CO2):

1. Using Web resources or documentation to which you have access, look up the detailed specifications of the Cisco PIX 500 series firewall. Determine what type of firewall it is and what implementation it is. Also note any specific advantages or disadvantages.
2. Analyze the environment of your academic institution. Is it a medium-sized network or enterprise? What types of users utilize the network? Are there multiple operating systems? Is there sensitive data that requires additional security? Based on the factors you analyze, write a brief essay describing the environment and recommending a firewall solution. Explain your recommendation.
3. Assume you are working for a small organization that has a moderate security budget. Select a particular IDS solution you would recommend for that organization. Write your

recommendations, including your reasons, in a memo format as if submitting them to a CIO or other decision maker.

Course Outcome 3 (CO3)

1. Find an encryption method that has been used historically but is no longer used (such as the Enigma cipher of the Germans in World War II). Describe how that encryption method works, paying particular attention to how it contrasts with more modern methods.
2. Using the Web or other resources look up each of the authentication protocols. Compare the protocols by pointing out the strengths and weaknesses of each. Which one would you recommend for your school, company, or organization? State the reasons behind your recommendation.
3. Unfortunately, technical strength is not the only criterion by which any solution is judged. Cost must be taken into account. For this project you will do cost estimates. This will require you to research product Web sites and perhaps even call sales representatives.
   - Assume a local area network that is small (under 100 users, 5 servers).
   - Assume 20 remote users, not all connected at the same time.
   - Assume an average of five to eight connections at any given time.
   - Research three solutions that can support this scenario, and report on the cost of each.

Course Outcome 4 (CO4)

1. Configure and setup Windows XP VPN Server and client
2. Using the Web or other resources find out specifics about the Encrypted File System that is part of Windows. Describe this file system, and any strengths and any weaknesses you find.
3. Using a laboratory Linux machine, accomplish the following: (I) Ensure that user accounts are set up securely. (II) Shut down unused and unneeded daemons. (III) Apply the Linux-specific settings

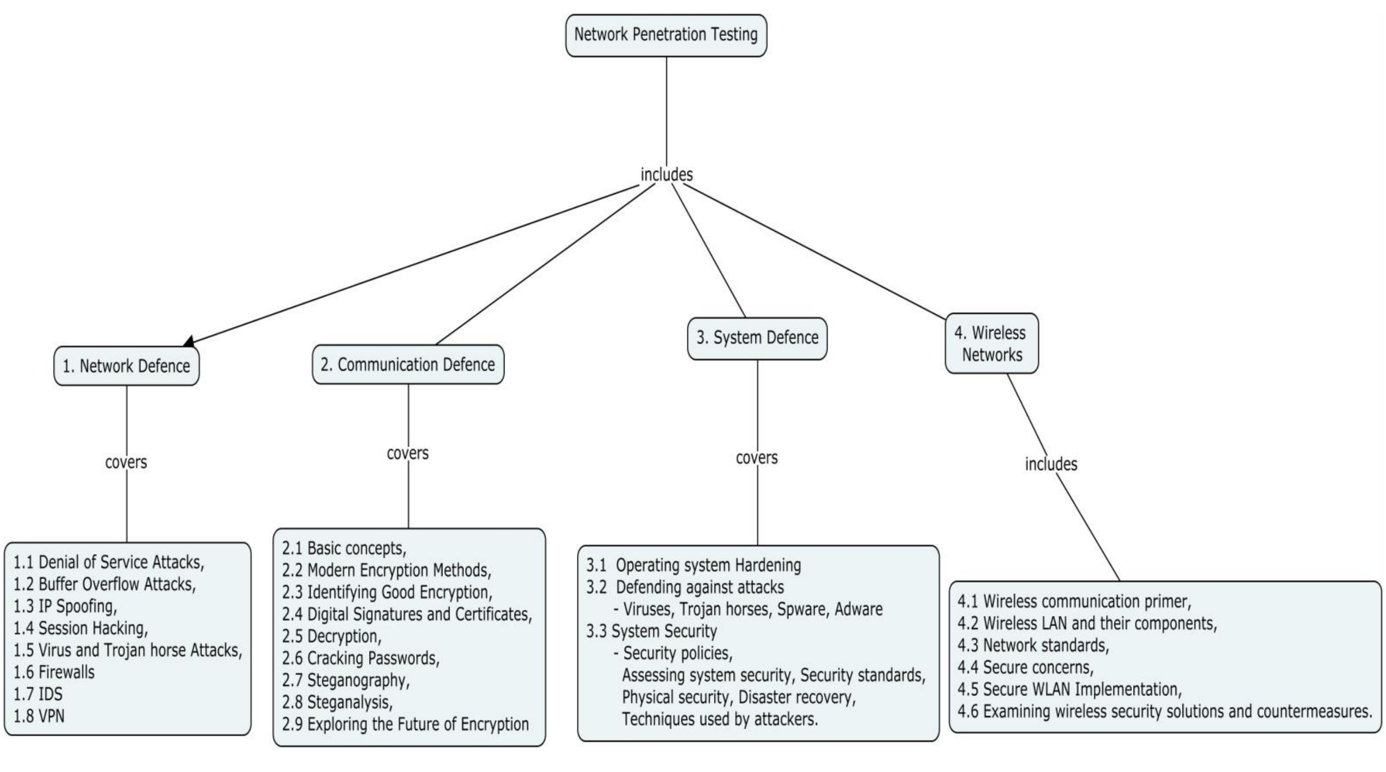
Course Outcome 5 (CO5)

1. Compare the features of four antivirus packages, paying particular attention to: Items that are unique to one solution. What each scanner picks up (i.e., if they are all used to scan the same folder, do they all detect the same items?).
2. Using the Web or other resources find out the following facts: How common are Trojan horse attacks? What effects do these have on businesses? What steps do you recommend to help reduce the threat of Trojan horse attacks?
3. Download one anti-spyware product. Install it on a lab machine and run it. Compare the results to what you got with Spy Sweeper.

Course Outcome 6 (CO6)

1. Ask a local business or your college for a copy of its security policies. Study the policies carefully. Summarize the main theme of these policy recommendations. Choose the policy recommendation you believe is the most secure, and state the reasons for your choice.
2. Find an organization that will allow you to review their security policies. You can try inquiring at any place you work, asking friends and relatives if you might check with their company's IT department, or checking with your college/university IT department. Make sure the organization has no objection to your review before you proceed. The organization you review should have written security policies. Summarize the organization's policies and make recommendations for changes you feel are needed to improve security there. You can also use resources that define appropriate security policies to compare against the policies of your chosen organization.
3. Using the Web and other resources, write a brief essay on the Common Criteria. Feel free to elaborate on areas that interest you, but your paper must address the following questions:
    - What is the current version being used?
    - When was it released?
    - How does this version define the scope of security?
    - What industry certifications use the common criteria?

Concept Map



Syllabus

Introduction: Basics of a Network, Network Utilities, OSI Model, TCP/IP, IPv4 Addressing, IPv6 Addressing, Assessing Likely Threats to the Network, Classifications of Threats, Likely Attacks, Threat Assessment, Security Terminologies, Choosing a Network Security Approach, Network Security and the Law, Security Resources .

Network Defence: Denial of Service Attacks, Buffer Overflow Attacks, IP Spoofing, Session Hacking, Virus and Trojan horse Attacks. Firewall – Basic concepts, Implementing Firewalls, Selecting and Using a Firewall, Proxy Servers, Single Machine Firewalls, User Account Control, Windows and Linux Firewalls, Small Office/Home Office Firewalls, Medium-Sized Network Firewalls, Enterprise Firewalls. IDS – Basic concepts, Implementing IDS Systems, Implementing Honey Pots. Virtual Private Networks - Basic VPN Technology, Using VPN Protocols for VPN Encryption, IPSec, SSL, Implementing VPN Solutions.

Communication Defense: Basic concepts, Modern Encryption Methods, Identifying Good Encryption, Digital Signatures and Certificates, Decryption, Cracking Passwords, Steganography, Steganalysis, Exploring the Future of Encryption.

System Defense: Basic concepts, Configuring Windows, Configuring Linux, Patching the Operating System, Configuring Browsers. Virus - Virus Scanners, Antivirus Policies and Procedures, Additional Methods for Defending the System, Procedure to defend against Virus infected system. Trojan Horses, Spyware, and Adware. Security policies, Assessing system security, Security standards, Physical security, Disaster recovery, Techniques used by attackers.

Wireless Network Defence: Wireless communication primer, Wireless LAN and their components, Network standards, Secure concerns, Secure WLAN Implementation, Examining wireless security solutions and countermeasures.

Text Book

1. Chuck Easttom, “Network Defense and Countermeasures: Principles and Practices”, Pearson education, Second edition, 2014.
2. Randy Weaver, Dawn Weaver, Dean Farwood, “Guide to Network Defense and Countermeasures”, Cengage Learning, Third edition, 2014.

References

1. E-council, “Network defence Architect” - http://www.eccouncil.org/Certification/certified-network-defense-architect.

Course Contents and Lecture Schedule

Module No.	Topic	No. of Lectures
0	**Introduction**	
0.1	Basics of a Network, Network Utilities,	1
0.2	OSI Model,	
0.3	TCP/IP -, IPv4 Addressing, IPv6 Addressing,	
0.4	Assessing Likely Threats to the Network,	1
0.5	Classifications of Threats,	
0.6	Likely Attacks,	1
0.7	Threat Assessment,	

Module No.	Topic	No. of Lectures
0.8	Security Terminologies,	1
0.9	Choosing a Network Security Approach,	
0.10	Network Security and the Law,	1
0.11	Security Resources.	
1	**Network Defence**	
1.1	Denial of Service Attacks,	1
1.2	Defending against Buffer Overflow Attacks,	
1.3	Defending against IP Spoofing,	1
1.4	Defending against Session Hacking,	
1.5	Blocking Virus and Trojan horse Attacks.	
1.6	Firewall – Basic concepts,	1
1.6.1	Implementing Firewalls,	
1.6.2	Selecting and Using a Firewall,	
1.6.3	Proxy Servers,	1
1.6.4	Single Machine Firewalls,	
1.6.5	User Account Control,	1
1.6.7	Windows and Linux Firewalls,	
1.6.8	Small Office/Home Office Firewalls,	
1.6.9	Medium-Sized Network Firewalls,	1
1.6.10	Enterprise Firewalls.	
1.7	IDS – Basic concepts,	1
1.7.1	Implementing IDS Systems,	
1.7.2	Implementing Honey Pots.	
1.8	Virtual Private Networks	1
1.8.1	Basic VPN Technology,	
1.8.2	Using VPN Protocols for VPN Encryption,	
1.8.3	IPSec,	1
1.8.4	SSL,	
1.8.5	Implementing VPN Solutions.	
2	**Communication Defence**	
2.1	Basic concepts,	2
2.2	Modern Encryption Methods,	
2.3	Identifying Good Encryption,	
2.4	Digital Signatures and Certificates,	1
2.5	Decryption, Cracking Passwords,	
2.6	Steganography,	2
2.7	Steganalysis,	
2.8	Exploring the Future of Encryption.	
3	**System Defence**	
3.1	Operating System Hardening	1
3.1.1	Basic concepts,	
3.1.2	Configuring Windows,	1
3.1.3	Configuring Linux,	1
3.1.4	Patching the Operating System,	1
3.1.5	Configuring Browsers.	
3.2	Defending against Attacks	1
3.2.1	Virus - Virus Scanners,	2

Module No.	Topic	No. of Lectures
3.2.2	Antivirus Policies and Procedures,	
3.2.3	Additional Methods for Defending the System,	
3.2.4	Procedure to defend against Virus infected system.	
3.2.5	Trojan Horses,	1
3.2.6	Spyware, and	2
3.2.7	Adware.	
3.3	System Security	1
3.3.1	Security policies,	
3.3.2	Assessing system security,	2
3.3.3	Security standards,	
3.3.4	Physical security,	
3.3.5	Disaster recovery,	
3.3.6	Techniques used by attackers.	1
4	**Wireless Networks**	
4.1	Wireless communication primer,	1
4.2	Wireless LAN and their components,	
4.3	Network standards,	1
4.4	Secure concerns,	
4.5	Secure WLAN Implementation,	1
4.6	Examining wireless security solutions and countermeasures.	
	Total Lectures	**36**

Course Designers:

1. Mr.M. Thangavel mtit@tce.edu
2. Mr.E. Ramanujam erit@tce.edu

14ISPK0	**COGNITIVE SCIENCES**	Category	L	T	P	Credit
		PE	3	1	0	4

Preamble

To understand contemporary theories, methods, and empirical findings about human cognition. To develop an ability to think scientifically about high-level cognitive processes.

Prerequisite

- NIL

Course Outcomes

On successful completion of the course, the students will be able to

Course Outcomes		Bloom's Level
CO1:	Understand the philosophy	Understand
CO2:	Define the adaptive nature of cognition	Understand
CO3:	Explain contrast detection in cognitive neuroscience	Understand
CO4:	Apply the cognitive approach to identify the autism child early detection	Apply
CO5:	Discuss the three classical philosophical issues of mind	Analyze

Mapping with Programme Outcomes

COs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11
CO1.	M	L	L								
CO2.	M	L	L								
CO3.	L	L	L								
CO4.	M	L	L					L	L		
CO5.	L	L	L						L	L	L

S- Strong; M-Medium; L-Low

Assessment Pattern

Bloom's Category	Continuous Assessment Tests			Terminal Examination
	1	2	3	
Remember	20	20	20	20
Understand	30	30	20	20
Apply	40	40	40	40
Analyze	10	10	20	20
Evaluate	-	-	-	-
Create	-	-	-	-

Course Level Assessment Questions

Course Outcome 1 (CO1):

1. What is the relation between the mental and the physical?
2. State the FOL support for logical representation and reasoning
3. Compare explanation based learning and case based reasoning

Course Outcome 2 (CO2):

1. Differentiate Episodic memory and Semantic memory
2. What are the stages of perceptual representation
3. List the advantages of knowledge based system

Course Outcome 3 (CO3):

1. Summarize the ways to do decision making under uncertainty
2. Discuss the sensory perceptual plasticity
3. Compare implicit and explicit memory

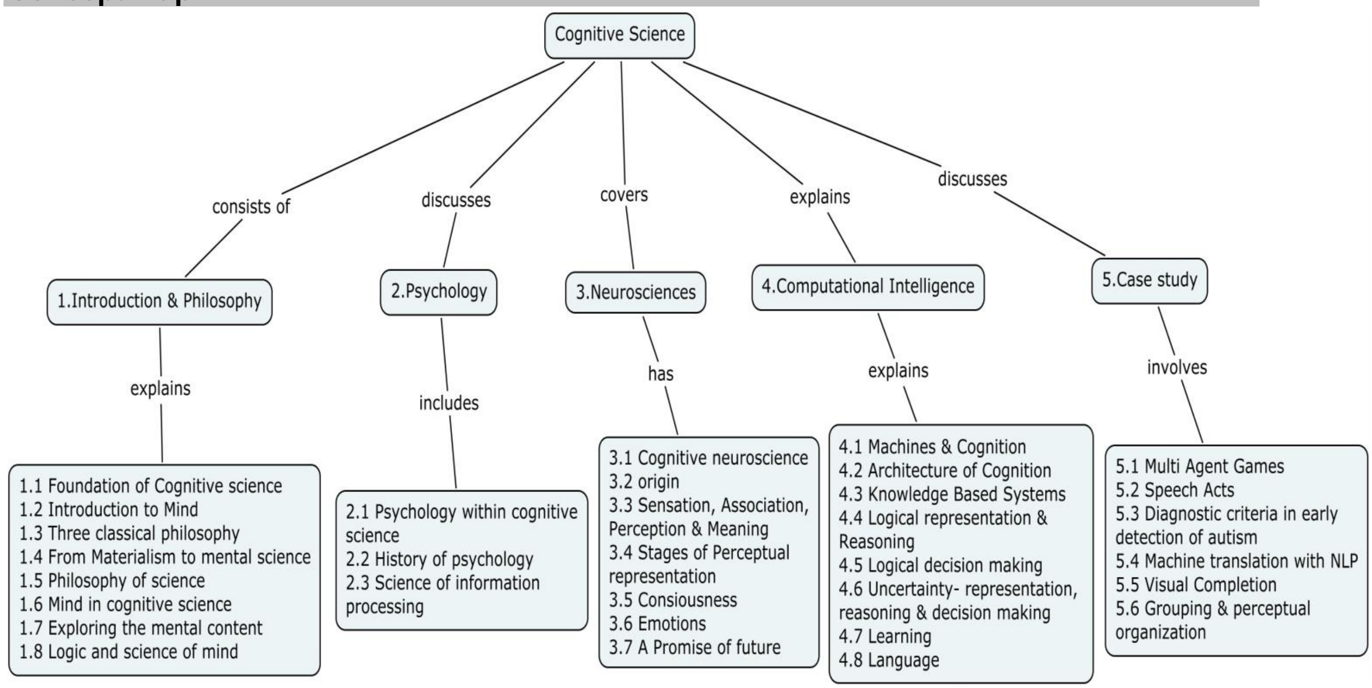
Course Outcome 4 (CO4):

1. Explain the dynamic control of sensitivity in the mature brain
2. Design the machine vision process using NLP
3. State the stages of perceptual representation

Course Outcome 5 (CO5):

1. Explain the ways to forming a decision to act
2. Discuss about consciousness and emotions role in patent recovery
3. Describe the transition from sensory processing to motor control

Concept Map



Syllabus

Introduction and Philosophy: Foundation of Cognitive Science – Introduction to Mind – three classical philosophy about mind – From materialism to mental science – philosophy of science - mind in cognitive Science – exploring the mental content – logic and science of mind

Psychology: The place of psychology within cognitive science – history of psychology – science of information processing

Neurosciences: Cognitive neuroscience – origin of cognitive neuroscience – sensation, association, perception and meaning – stages of perceptual representation –consciousness-emotions – a promise of future

Computational Intelligence: Machines and cognition – architectures of cognition – knowledge based systems – logical representation and reasoning –logical decision making – representation and reasoning under uncertainty – decision making under uncertainty – learning – language

Case Study: Multi Agent Games – Speech Acts – Diagnostic Criteria in early detection of autism – Understanding in Machine Translation with NLP (Natural Language Processing) – visual completion - grouping and perceptual organization

Text Books

1. Wilson, Robert A., & Keil, Frank C. (eds.), The MIT Encyclopedia of the Cognitive Sciences (MITECS), MIT Press, 2001

References

1. Bowerman, Melissa and Stephen C. Levinson, Language Acquisition and Conceptual Development, Cambridge University Press 2001.
2. Sternberg, Robert J., Cognitive Psychology, 4th ed., Cengage Learning India, 2008.
3. Gardenfors, Peter, Conceptual Spaces: The Geometry of Thought, MIT Press, 2000, 317 pages.

Course Contents and Lecture Schedule

Module No	Topic	No. of Lectures
1	**Introduction and Philosophy**	
1.1	Foundation of Cognitive Science	1
1.2	Introduction to Mind	1
1.3	Three classical philosophy about mind	1
1.4	From materialism to mental science	1
1.5	Philosophy of science	1
1.6	Mind in cognitive Science	1
1.7	Exploring the mental content	1
1.8	Logic and science of mind	1
2	**Psychology**	
2.1	The place of psychology within cognitive science	1
2.2	History of psychology	1
2.3	Science of information processing	2
3	**Neurosciences**	
3.1	Cognitive neuroscience	1
3.2	Origin of cognitive neuroscience	1
3.3	Sensation, Association, Perception and Meaning	2
3.4	Stages of perceptual representation	2

3.5	Consciousness	1
3.6	Emotions	1
3.7	A promise of future	1
4	**Computational Intelligence**	
4.1	Machines and cognition	1
4.2	Architectures of cognition	2
4.3	Knowledge based systems	1
4.4	Logical representation and reasoning	1
4.5	Logical decision making	1
4.6	Representation and reasoning under uncertainty – decision making under uncertainty	1
4.7	Learning	1
4.8	Language	1
5	**Case Studies**	
5.1	Multi Agent Games	1
5.2	Speech Acts	1
5.3	Diagnostic Criteria in early detection of autism.	1
5.4	Understanding in Machine Translation with NLP (Natural Language Processing)	1
5.5	Visual completion	1
5.6	Grouping and perceptual organization	1
	Total Lectures	**36**

Course Designers:

1. Dr.D.Tamilselvi dtamilselvi@tce.edu
2. Ms.T.Manju tmanju@tce.edu

OUTCOME BASED EDUCATION

CURRICULUM AND DETAILED SYLLABI

FOR

M.E. COMPUTER SCIENCE AND INFORMATION SECURITY DEGREE PROGRAMME

TWO CREDIT COURSES

FOR THE STUDENTS ADMITTED IN THE

ACADEMIC YEAR 2016-17 ONWARDS

THIAGARAJAR COLLEGE OF ENGINEERING
(A Government Aided ISO 9001:2008 certified Autonomous Institution affiliated to Anna University)
MADURAI – 625 015, TAMILNADU

Phone: 0452 – 2482240, 41
Fax: 0452 2483427
Web: www.tce.edu

Passed in Board of Studies Meeting on 29.04.2016 Approved in Academic Council Meeting on 18.06.2016

LIST OF TWO CREDIT COURSES

S. No.	COURSE CODE	COURSE NAME
1	14IS2A0	MALICIOUS SOFTWARE ANALYSIS
2	14IS2B0	ADVANCES IN NETWORK SECURITY AND MANAGEMENT

14IS2A0	MALICIOUS SOFTWARE ANALYSIS	Category	L	T	P	Credit
		PE	2	0	0	2

Preamble

This course explores malware analysis tools and techniques in depth. Understanding the capabilities of malware is critical to an organization's ability to derive threat intelligence, respond to information security incidents, and fortify defenses. This course builds a strong foundation for reverse-engineering malicious software using a variety of system and network monitoring utilities, a disassembler, a debugger, and other tools useful for turning malware inside-out.

Prerequisite

- 14IS120 - Cryptography
- 14IS130 - Network Security
- 14IS210 - System Security

Course Outcomes

On the successful completion of the course, students will be able to

Course Outcomes		Bloom's Level
CO1:	Explain the characteristics of Malware and its effects on Computing systems.	Understand
CO2:	Practice the given system scenario using the appropriate tools to Identify the vulnerabilities and to perform Malware analysis.	Apply
CO3:	Analyze the given Portable Executable and Non-Portable Executable files using Static and dynamic analysis techniques.	Analyze

Mapping with Programme Outcomes

COs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11
CO1	L										
CO2	M	M			L						
CO3	S	S	M		M	M		M	M	L	

S- Strong; M-Medium; L-Low

Assessment Pattern

Bloom's Category	CAT - I	Terminal Examination
Remember	-	20
Understand	-	30
Apply	40	50
Analyse	60	0
Evaluate	-	0
Create	-	0

- CAT – 1 is used to evaluate the CO2 and CO3 in 40% and 60% respectively through Lab Assessment
- Terminal Examination is used to evaluate CO1, CO2 and CO3 through written examination.

Course Level Assessment Questions

Course Outcome 1 (CO1):

1. Define Malware
2. List the types of Malware Anaysis.
3. State the need and types of Malware Analysis
4. State the reason for Malware Analysis in the online webpages.
5. Compare the PE and Non-PE Structure.
6. Describe the use of YARA Rules in Dynamic Analysis
7. Give the working principle for Anti-virus.

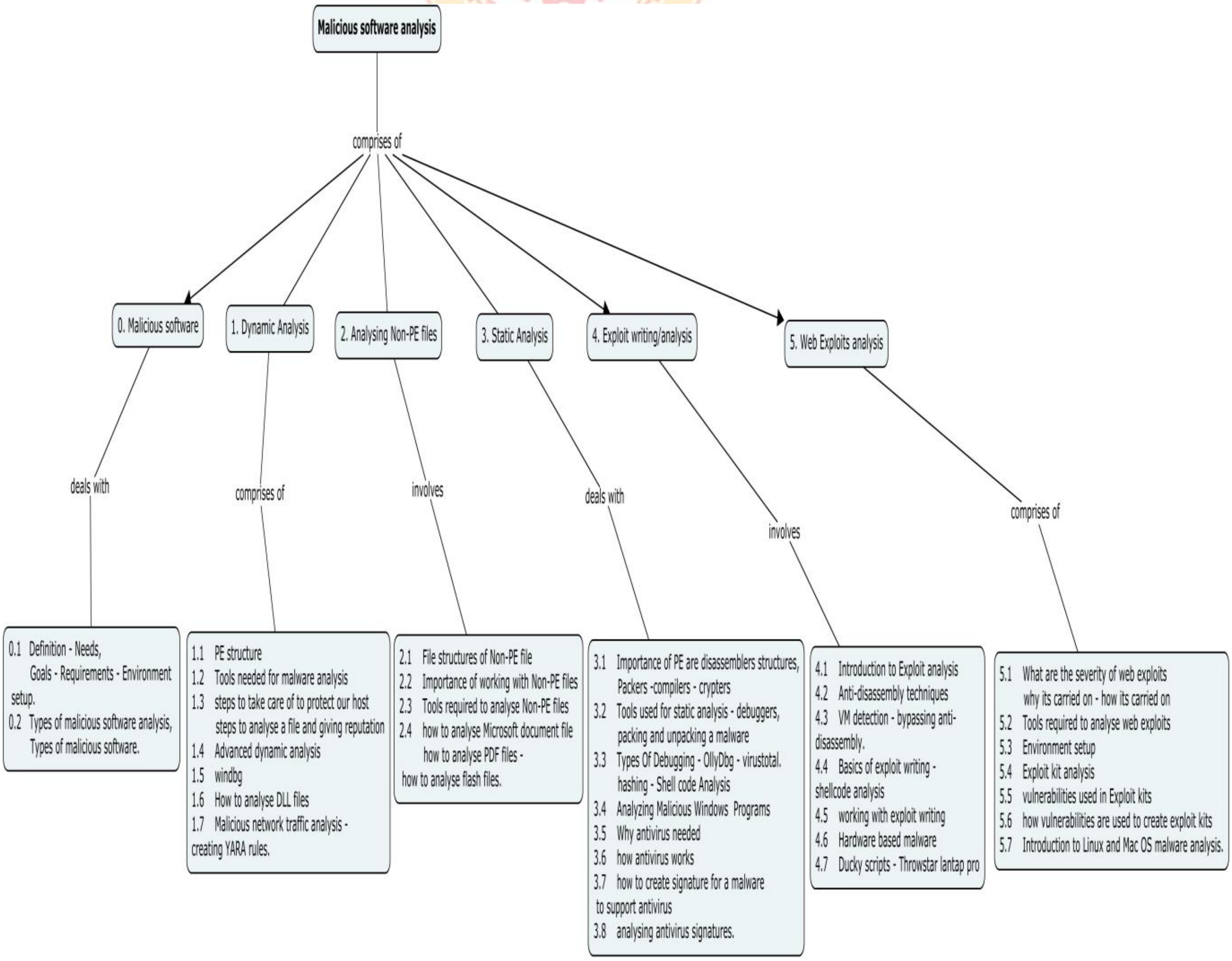
Course Outcome 2 (CO2):

1. Illustrate with suitable example, how to create YARA rules.
2. Apply suitable Malware analysis, through which malware signature can be created for Anti-virus.
3. Distinguish the use of Static and Dynamic Analysis in Malware applications.
4. Compare the application of Web exploits in Malware

Course Outcome 3 (CO3)

Analyze the Banking application for the possible vulnerabilities and perform Malware analysis using, FakeAV malware, ZeroAccess Rootkit, Ransomware, DLL malware and Trojan.

Concept Map



Syllabus

Malicious software: Definition - Needs - Goals - Requirements - Environment setup - Types of malicious software analysis, Types of malicious software.

Dynamic Analysis: PE structure - Tools needed for malware analysis - steps to take care of to protect our host - steps to analyse a file and giving reputation - Advanced dynamic analysis - windbg - How to analyse DLL files - Malicious network traffic analysis - creating YARA rules.

Analysing Non-PE files: File structures of Non-PE file - Importance of working with Non-PE files - Tools required to analyse Non-PE files - how to analyse Microsoft document file - how to analyse PDF files - how to analyse flash files.

Static Analysis: Importance of PE are disassemblers structures - Packers -compilers - crypters - Tools used for static analysis - debuggers - packing and unpacking a malware - Types Of Debugging - OllyDbg - virustotal - hashing - Shell code Analysis - Analyzing Malicious Windows Programs - Why antivirus needed - how antivirus works - how to create signature for a malware to support antivirus - analysing antivirus signatures.

Exploit writing/analysis: Introduction to Exploit analysis - Anti-disassembly techniques - VM detection - bypassing anti-disassembly - basics of exploit writing - shellcode analysis - working with exploit writing - Hardware based malware - Ducky scripts - Throwstar lantap pro.

Web Exploits analysis: What are the severity of web exploits - why its carried on - how its carried on - tools required to analyse web exploits - Environment setup -Exploit kit analysis - vulnerabilities used in Exploit kits - how vulnerabilities are used to create exploit kits - Introduction to Linux and Mac OS malware analysis.

Hands-on Topics:

1. Live analysis on FakeAV malware, DLL malware samples and ZeroAccess Rootkit.
2. Practical session on Ransomware and FakeAv for trainees.
3. Practical session on Trojan.RAT dll file, Pony loader malware, mass-mailer worm, zbot trojan for trainees.
4. Live analysis on Microsoft document file embedded with malware
5. Practical session on w97m.downloader, OLE component w97m.downloader malware.
6. Analysis of suspicious JPG file.
7. Practical session on JPG malware analysis.
8. Live analysis on PDF file embedded with malware
9. Practical session on DOC,PDF malware files for trainees.
10. Live session on static analysis of a malware sample (PlugX rat), basic exploit writing.
11. Practical session on static analysis of a Netsky worm for trainees, static analysis of packers
12. Practical session on exploit writing, hardware based malware, JavaScript malwares, creating signature for a malware, analysing web exploits for trainees.
13. Live analysis of Web exploits, antivirus signature creation.
14. YARA rules creation.
15. Live session on exploiting vulnerabilities in a program, windows vulnerability and installing Ransomware

Textbook

1. Michael Sikorski and Andrew Honig, "Practical Malware Analysis" ,No starch press, February, 2012.
2. Michael Ligh, Steven Adair, Blake Hartstein, Matthew Richard , "Malware Analyst's Cookbook" , John Wiley & Sons, October, 2010.
3. Mark Russinovich, David A. Solomon, Alex Ionescu "Windows Internals", Microsoft Press, 6th edition, 2012.

4. Abraham Silberschatz , Peter B. Galvin, Greg Gagne, "Operating System Concepts", John Wiley & Sons, Inc., 9th edition, 2015.

Web References

1. http://opensecuritytraining.info/ReverseEngineeringMalware.html
2. https://zeltser.com/reverse-malware-cheat-sheet/
3. http://arteam.accessroot.com/arteam/site/download.php?view.112
4. https://tuts4you.com/download.php?list.17
5. https://technet.microsoft.com/en-in/sysinternals/bb963901.aspx
6. http://www.sans.org/reading-room/whitepapers/malicious/malware-analysis-introduction-2103/.git/HEAD
7. https://zeltser.com/build-malware-analysis-toolkit/

Course Contents and Lecture Schedule

Module .No	Topics	No. of Lectures
0.	**Malicious software**	
0.1	Definition - Needs - Goals - Requirements - Environment setup.	1
0.2	Types of malicious software analysis, Types of malicious software.	
1.	**Dynamic Analysis**	
1.1	PE structure	1
1.2	Tools needed for malware analysis	
1.3	steps to take care of to protect our host - steps to analyse a file and giving reputation	1
1.4	Advanced dynamic analysis	
1.5	windbg	1
1.6	How to analyse DLL files	
1.7	Malicious network traffic analysis - creating YARA rules.	1
2.	**Analysing Non-PE files**	
2.1	File structures of Non-PE file	1
2.2	Importance of working with Non-PE files	1
2.3	Tools required to analyse Non-PE files	
2.4	how to analyse Microsoft document file - how to analyse PDF files - how to analyse flash files.	2
3.	**Static Analysis**	
3.1	Importance of PE are disassemblers structures - Packers - compilers - crypters	2
3.2	Tools used for static analysis - debuggers - packing and unpacking a malware	
3.3	Types Of Debugging - OllyDbg - virustotal - hashing - Shell code Analysis	2
3.4	Analyzing Malicious Windows Programs	
3.5	Why antivirus needed	3
3.6	how antivirus works	
3.7	how to create signature for a malware to support antivirus	
3.8	analysing antivirus signatures.	

4.	**Exploit writing/analysis**	
4.1	Introduction to Exploit analysis	1
4.2	Anti-disassembly techniques	
4.3	VM detection - bypassing anti-disassembly.	2
4.4	Basics of exploit writing - shellcode analysis	
4.5	working with exploit writing	2
4.6	Hardware based malware	
4.7	Ducky scripts - Throwstar lantap pro	
5.	**Web Exploits analysis**	
5.1	What are the severity of web exploits - why its carried on - how its carried on	1
5.2	Tools required to analyse web exploits	1
5.3	Environment setup	1
5.4	Exploit kit analysis	1
5.5	vulnerabilities used in Exploit kits	1
5.6	how vulnerabilities are used to create exploit kits	1
5.7	Introduction to Linux and Mac OS malware analysis.	1
Total Lecture Hours		**28**

Course Designers:

1. Ms..J.Reegun Richard — reegunj@outlook.com

   Industry : Symantec Corporation, India

   Area of Interests : Vulnerability researching in windows and web application penetration testing, analysing targeted attacks like exploit kits, Dynamic& static analysis of malware, Network traffic analysis, Adding rules to malicious network traffic, detailed analysis on malicious network traffic to get the URI patterns for exploit kits and targeted attacks, Expertise in removing malwares/rootkits manually.

2. Ms.M.Thangavel — thangavelmuruganme@gmail.com / mtit@tce.edu

14IS2B0	ADVANCES IN NETWORK SECURITY AND MANAGEMENT	Category	L	T	P	Credit
		PE	2	0	0	2

Preamble

Network management and security are essential factors in the reliable, efficient, and secure operation of networks. As businesses become increasingly dependent on networking services, keeping these services running and secure becomes synonymous with keeping the business running. This course provides a thorough introduction to network management technologies and standards as well as to a wide variety of techniques for evaluating, monitoring, and defending the security of computer networks and systems. This course provides the fundamental knowledge to analyze risks to the system and implement a workable security policy that protects the information assets from potential intrusion, damage or theft. Topics include secure routing and switching, Firewall technologies, VPN Technology, Intrusion Prevention/Detection systems.

Prerequisite

14IS130 - Network Security

Course Outcomes

On the successful completion of the course, students will be able to

Course Outcomes		Bloom's Level
CO1	Examine the need of security for the given network scenario.	Apply
CO2	Criticize the preventive measures to secure routing and switching.	Analyze
CO3	Infer the design of firewall, VPN and IDS / IPS for the given network.	Analyze

Mapping with Programme Outcomes

COs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11
CO1	M	M			L						
CO2	S	S	M		M	M		M	M	L	S
CO3	S	S	M		M	M		M	M	L	S

S- Strong; M-Medium; L-Low

Assessment Pattern

Bloom's Category	CAT - I	Terminal Examination
Remember	-	20
Understand	-	30
Apply	40	50
Analyse	60	0
Evaluate	-	0
Create	-	0

- CAT – 1 is used to evaluate the CO2, CO3 in 40%, 60% respectively through Lab Assessment
- Terminal Examination is used to evaluate CO1, CO2, CO3 through written examination.

Course Level Assessment Questions

Course Outcome 1 (CO1):

1. Infer the importance of CIA in Network security.
2. Relate Network attack methods and vectors.
3. Outline the importance of Network security for a virtual environment
4. Explain data loss and exfiltration methods
5. Interpret good security practices for network management.

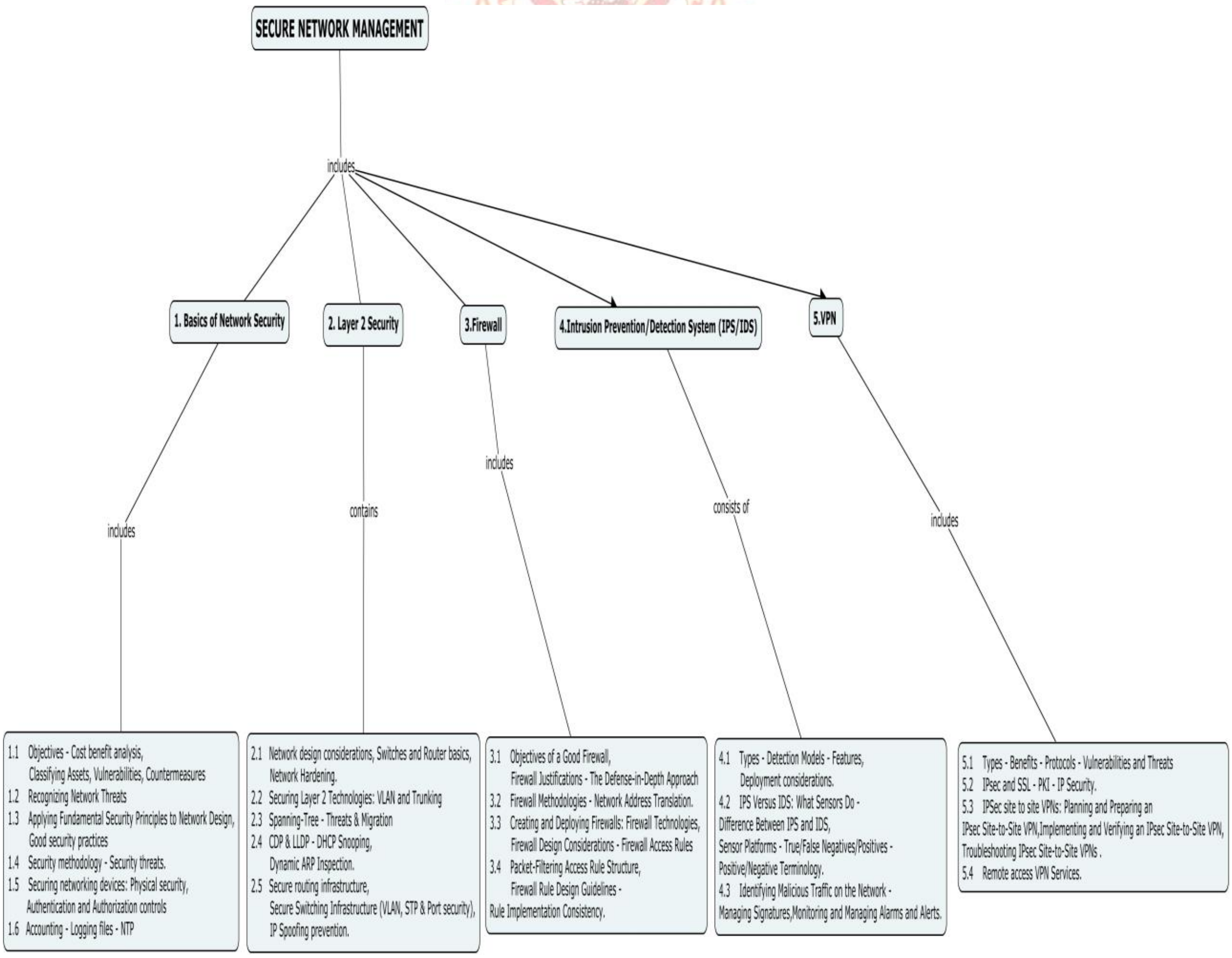
Course Outcome 2 (CO2):

1. Illustrate trunking with 802.1Q.
2. Identify the best practices and security toolkit to migrate from common layer 2 threats.
3. Develop an s secure routing infrastructure between two different organizations.
4. Model secure switching infrastructure for any educational organization.
5. Utilize the IP Spoofing prevention techniques to solve the network security threats and attacks.

Course Outcome 3 (CO3):

1. Analyze the configuration of IPSec for the simulated network.
2. Inspect the troubleshooting steps of IPsec Site-to-Site VPNs in Cisco IOS
3. Examine the Firewall rules in a Desktop computer.
4. Identify the Malicious traffic in the network using appropriate tools.
5. Simplify the steps for monitoring and managing the alerts and alarms

Concept Map



Syllabus

Basics of Network Security: Objectives - Cost benefit analysis - Classifying Assets, Vulnerabilities, Countermeasures - Recognizing Network Threats - Applying Fundamental Security Principles to Network Design - Good security practices - Security methodology - Security threats. Securing Networking Devices: Physical security - Authentication and Authorization controls - Accounting - Logging files - NTP.
Layer 2 security: Network design considerations - Switch and Router basics - Network Hardening. Securing Layer 2 Technologies: VLAN and Trunking - Spanning-Tree - Threats & Migration - CDP & LLDP - DHCP Snooping - Dynamic ARP Inspection. Secure routing infrastructure - Secure Switching Infrastructure (VLAN, STP & Port security) - IP Spoofing prevention.
Firewall: Objectives of a Good Firewall - Firewall Justifications - The Defense-in-Depth Approach - Firewall Methodologies - Network Address Translation. Creating and Deploying Firewalls: Firewall Technologies - Firewall Design Considerations - Firewall Access Rules - Packet-Filtering Access Rule Structure - Firewall Rule Design Guidelines - Rule Implementation Consistency.
Intrusion Prevention/Detection System (IPS/IDS): Types - Detection Models - Features - Deployment considerations. IPS Versus IDS: What Sensors Do - Difference Between IPS and IDS - Sensor Platforms - True/False Negatives/Positives - Positive/Negative Terminology. Identifying Malicious Traffic on the Network - Managing Signatures - Monitoring and Managing Alarms and Alerts.
VPN Technology: Types - Benefits - Protocols - Vulnerabilities and Threats - IPsec and SSL - PKI - IP Security. IPSec site to site VPNs: Planning and Preparing an IPsec Site-to-Site VPN - Implementing and Verifying an IPsec Site-to-Site VPN - Troubleshooting IPsec Site-to-Site VPNs . Remote access VPN Services.

Textbook

1. John Stuppi, Omar Santos, "CCNA Security 210-260 Official Cert Guide", Publisher: Cisco Press, ISBN: 9780134077857, Release Date: September 2015.
2. Mark Rhodes-Ousley, Roberta Bragg, Keith Strassberg, " Network Security: The Complete Reference", Publisher: McGraw-Hill Osborne Media, Edition: First, Released: October, 2013

References

1. Joseph Migga Kizza, “Computer Network Security”, Springer, 2005.
2. Douglas R. Stinson, “Cryptography Theory and Practice”, Third Edition, Chapman & Hall/CRC, 2006
3. William Stallings, “Network Security Essentials Applications and Standards”, Pearson Education, Fourth Edition, 2011
4. William Stallings, Lawrie Brown, “Computer Security: Principles and Practice”, First Edition, 2008.
5. “VPN Security”, The Government of the Hong Kong Special Administrative Region 2008.

Course Contents and Lecture Schedule

Module. No	Topics	No. of Lectures
1	**Basics of Network Security**	
1.1	Objectives - Cost benefit analysis - Classifying Assets, Vulnerabilities, Countermeasures	1
1.2	Recognizing Network Threats	1
1.3	Applying Fundamental Security Principles to Network Design - Good security practices	1

1.4	Security methodology - Security threats.	1
1.5	Securing Networking Devices - Physical Security - Authentication and Authorization controls	1
1.6	Accounting - Logging files - NTP	1
2	**Layer 2 Security**	
2.1	Network design considerations - Switch and Router basics - Network Hardening.	1
2.2	Securing Layer 2 Technologies: VLAN and Trunking	1
2.3	Spanning-Tree - Threats & Migration	1
2.4	CDP & LLDP - DHCP Snooping - Dynamic ARP Inspection.	1
2.5	Secure routing infrastructure - Secure Switching Infrastructure (VLAN, STP & Port security) - IP Spoofing prevention.	2
3	**Firewall**	
3.1	Objectives of a Good Firewall - Firewall Justifications - The Defense-in-Depth Approach	1
3.2	Firewall Methodologies - Network Address Translation.	1
3.3	Creating and Deploying Firewalls: Firewall Technologies - Firewall Design Considerations - Firewall Access Rules	2
3.4	Packet-Filtering Access Rule Structure - Firewall Rule Design Guidelines - Rule Implementation Consistency.	2
4	**Intrusion Prevention/Detection System (IPS/IDS)**	
4.1	Types - Detection Models - Features - Deployment considerations.	1
4.2	IPS Versus IDS: What Sensors Do - Difference Between IPS and IDS - Sensor Platforms - True/False Negatives/Positives - Positive/Negative Terminology.	1
4.3	Identifying Malicious Traffic on the Network - Managing Signatures - Monitoring and Managing Alarms and Alerts.	2
5	**VPN Technology**	
5.1	Types - Benefits - Protocols - Vulnerabilities and Threats	1
5.2	IPsec and SSL - PKI - IP Security.	1
5.3	IPSec site to site VPNs: Planning and Preparing an IPsec Site-to-Site VPN - Implementing and Verifying an IPsec Site-to-Site VPN - Troubleshooting IPsec Site-to-Site VPNs .	2
5.4	Remote access VPN Services.	2
Total Lecture Hours		**28**

Course Designers:

1.	Manigandan Sellamuthu		sendmanigandan@gmail.com
	Industry	:	Symantec Corporation, India
	Profile	:	His professional background includes more than 12 years of experience as Network & Information Security Engineer with extensive technical and project management skills. He currently Holding various vendor certification such SANS - (GCIA,GCIH,GSSEC), Checkpoint - (CCSA,CCSE), Cisco -(CCSP,CCIE-Written), Sourcefire -(SFCP).
2.	Thangavel M		thangavelmuruganme@gmail.com / mtit@tce.edu