JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY ANANTHAPURAMU

COLLEGE OF ENGINEERING (AUTONOMOUS):: PULIVENDULA

Department of Computer Science & Engineering

LESSON PLAN

Course Title	:	**Information Security**			
Course Code	:	**15ACS81**			
Course Structure	:	Lectures	Tutorials	Practicals	Credits
		3	1	0	3
Course Coordinator	:	Mr.T.Niranjan Babu, Assistant Professor (Adhoc)			
Team of Instructors	:	Mr.G.Murali (HOD)			

I. Course Overview

The course helps the students to develop the algorithms for implementation of specific problem through different computer languages. This Information security course introduces students to the basics of the field. Students study monitors and protection procedures pertaining to security activities and learn to apply them practically. The hands-on practice involves protecting work with passwords and applying multiple security models and systems. Through these different programs, students learn how to identify security issues and protect information as well as track down those who steal that data. Because information security is necessary for homeland security and so many other fields, there are several types of programs available that vary in scope and focus. This course also dives into the very beginnings of cryptography. The course is implemented through lecture, tutorial and various assignments.

II. Prerequisite(s):

Level	Credits	Periods / Week	Prerequisites
UG	3	5	Computer Networks, S/W Engineering

III. Assessment:

FORMATIVE ASSESMENT	
Mid Semester Test I for 30 Marks in first 2 units is conducted at the starting of 9th week. Mid Semester Test II for 30 Marks in next 3 is conducted at the end of the course work. 80% for better mid marks and 20% for the other shall be considered as internal/mid test marks.	30 Marks
Total (Formative)	30 Marks
SUMMATIVE ASSESMENT	
End Semester Examination in all units is conducted for 70	70 marks

Marks	
Grand Total	100 Marks

IV. Course objectives:

This course focuses on how to design and build secure systems with a human-centric focus. We will look at basic principles of human-computer interaction, and apply these insights to the design of secure systems with the goal of developing security measures that respect human performance and their goals within a system

1. To introduce students with basic concepts in information system and its relevance in modern society.
2. To understand several security requirements and operations - analysis, design, and implementation of the Security System Development Life Cycle (Sec SDLC)
3. To understand and implement authentication, integrity and confidentiality along with related protocols.
4. Develop a basic understanding of cryptography, how it has evolved and some key encryption techniques used today.
5. To develop an understanding of security policies, as well as protocols to implement such policies in the form of message exchanges.

V. Course Outcomes:

Upon completion of this course, students will acquire knowledge about:

1. Provide security of the data over the network.

2. To do research in the emerging areas of cryptography and network security.

3. Implement various networking protocols.

4. Protect any network from the threats in the world.

5. To master information security governance, and related legal and regulatory issues.

6. To be familiar with how threats to an organization are discovered and analyzed.

7. To be familiar with advanced security issues and technologies.

8. To be familiar with network security threats and counter measures.

VI. Program outcomes:

a. An ability to apply knowledge of problem solving, mathematical foundations, algorithmic principles, and computer science and engineering theory in solving the computer-based systems to real-world problems (fundamental engineering analysis skills).
b. An ability to understand to write the algorithms, as well as to analyze and interpret the computer problems (information retrieval skills).
c. An ability to design , implement, and evaluate a computer-based system, process, component, module or program to meet desired needs, within realistic constraints such as economic, environmental, social, political, health and safety, manufacturability, and sustainability (Creative Skills) requirements.
d. An ability to function effectively on multi-disciplinary teams (team work).
e. An ability to analyze a problem, identify, formulate and use the appropriate computing and engineering requirements for obtaining its solution (engineering problem solving skills).
f. An understanding of professional, ethical, legal, security and social issues and responsibilities (professional integrity).
g. An ability to communicate effectively both in writing and orally (speaking / writing skills) with customers (stakeholders).
h. The broad education necessary to analyze the local and global impact of computing and engineering solutions on individuals, organizations, and society (engineering impact assessment skills).
i. Recognition of the need for, and an ability to engage in continuing professional development and life-long learning (continuing education awareness).
j. A Knowledge of contemporary issues (social awareness).
k. An ability to use current techniques, skills, and tools necessary for computing and engineering practice (practical engineering analysis skills).
l. An ability to apply design and development principles in the construction of software and hardware systems of varying complexity (software hardware interface).
m. An ability to recognize the importance of professional development by pursuing postgraduate studies or face competitive examinations and research works that offer challenging and rewarding careers in computing (successful career and immediate employment).

VII. Syllabus:

UNIT- I:

Introduction

History, critical characteristics, components, approaches of implementation, security systems development life cycle, security professionals.

Security Issues:

Need for security, threat, risk, attack, legal and ethical issues.Legal, Ethical and Professional Issues: law and ethics in information security, relevant u.s laws-international laws and legal bodies, ethics and information security**.**

UNIT- II

Security technology-firewalls and VPNs: physical design, firewalls, protecting remote connections.Planning for security: security policy, standards and practices, security blue print, security education, continuity strategies.

UNIT- III

Security technology-intrusion detection: access control and other security tools - intrusion detection and prevention systems, scanning and analysis tools, biometric access controls.

Cryptography: foundations of cryptology, cipher methods, cryptographic algorithms, cryptographic tools, protocols for secure communications, attacks on cryptosystems.

UNIT- IV

Electronic mail security:

Pretty Good Privacy (PGP); S/MIME

Security tools:

Intrusion detection systems, honey pots, honey nets and padded cell systems, scanning and
Analysis tools.

UNIT- V

Implementing information security: information security project management, technical topics of implementation, non-technical aspects of implementation, security certification and accreditation.

Security and personnel: positioning and staffing security function, credentials of information security professionals, internal control strategies.

Information security maintenance: security management models, the security maintenance model, digital forensics.

Course Outcomes:

1. *Aware of information security issues and understand its technologies.*
2. *Able to discover, analyse and deal with threads using advanced security issues and technologies.*
3. *Understand the current legal issues towards information security.*

TEXT BOOKS:

1. Michael e. Whitman, h j mattord , 2nd edition principals of information security,Thompson course technology, 2007.
2. **Cryptography and Network Security** Principles and Practices, Fourth Edition. By **William Stallings**
3. Michael e. Whitman and hebert j mattord, "principles of information security", fourth edition, cengage learning 2011.
4. Behrouz a forouzan, debdeepmukhopadhyay, cryptography and network security, 2nd Edition, tatamcgraw hill education private limited , new delhi, 2012.

REFERENCES:

1. Thomas r peltier, justingpeltier, john blackley, "information security fundamentals", auerbacj publications 2010.
2. Detmar w straub, seymorgoodman, richard l baskerville, "information security policy proceses and practices", phi, 2008.
3. Marks merkow and jimbreithaupt, "information security principle and practices", pearson education, 2007.
4. Kaufman, perlman , speciner 'network security' phi ,india, 2nd ed. 2010
5. **Online references** :
   http://www.cryptogram.org

VIII.Course Plan:

Lecture No.	Date	Course Learning Outcomes	Topics to be covered	Course Outcomes	Reference
UNIT-I	**Introduction to Information Security**				
1	02-12-2019	History of Information security	Introduction to IS	After completion of this unit students will acquire the knowledge about how to master the information security governance, and related legal and regulatory issues.	T1:1 T2:1.4
2	03-12-2019	critical characteristics	Basic characteristics of IS		T1:1.2
3	05-12-2019	components	To study about the different services of IS		T1:1.3
4	06-12-2019	security systems development life cycle	To study about life cycle of security systems development		T1:1.4 T2:2
5	09-12-2019	security professionals	To study about different security professionals and organizations		T1:1.5
6	10-12-2019	Need for security	To study the necessities of IS		T1:1.6
7	12-12-2019	threats, risks and attacks	To study about differences in between threats, risks and attacks		T1:2.1
8	13-12-2019	legal and ethical issues	To learn about various legal and ethical issues		T1:2.2
9	16-12-2019	international laws and legal bodies	To study about the legal bodies of information security		T1:2.3
10	17-12-2019	Viruses and worms	To study about the differences between viruses and worms		T1:2.4
					T1:2.6
UNIT -II	**Security Technology**			After completion of this unit students will obtain	T1:2.7
11	19-12-2019	Firewalls	Definition and types of firewalls		T1:2.8
12	20-12-2019	Virtual Private Networks	To study about the applications of VPN's		T1:2.9
13	23-12-	protecting remote connections	To study about the remote connections		

	2019			the knowledge regarding how to secure a system by using various techniques .	
14	24-12-2019	security policy, standards and practices	To study about different security policies		T1: 3.1
15-16	26-12-2019	security blue print	To study about various security systems architectures		T1:3.2
17-18	27-12-2019	security education	Security education for example cryptology etc.		T1.3.3
UNIT-III	**Security technology-intrusion detection**				T1:3.4
19-20	30-12-2019	intrusion detection and prevention systems	To study various intrusion detection systems	Students will get the specific knowledge about biometric access controls and encryption and decryption methods for different ciphers	T1:3.5
21-22	31-12-2019	scanning and analysis tools	To study about different virus scanning strategies		T1:3.7
23-24-25	02-01-2020	biometric access controls	biometric access controls and procedures		T1:3.8
26-27	03-12-2020	Introduction to Cryptography	History of cryptosystems		T1:4.1
28-29	06-01-2020	cipher methods	Types of Ciphers and techniques		T1:4.2-T2:3.7
30-31-32	07-01-2020	cryptographic algorithms	To study about various algorithms		T1:4.3
UNIT_IV	**Electronic mail security and Security tools**				T1:4.4 T2-3.9
33-34-35	09-01-2020	Pretty Good Privacy	To study about PGP policy	After completion of this unit they can able to solve security related problem and knowledge about PGP privacy.	T1:4.5
36-37	10-01-2020	Intrusion detection systems	Intrusion detection systems applications		T1:4.6
38-39	21-02-2020	honey nets and padded cell systems	Padded cell system concepts		T1.4.7 T2:3.12
40-41-42	23-02-2020	scanning and Analysis tools	To study about various scanning and analysis tools		T1:5.1
UNIT-V	**Implementing information security**				T1:5.6
43-44	02-03-2020	information security project management	To study about how manage the information security projects	Students may get	

				the knowledge for solving any problem i.e; a case study regarding any informatio n security systems.	
45-46	03-03-2020	technical topics of implementation	Implementation of IS technically		T1:5.8
47-48	09-03-2020	non-technical aspects of implementation	To design non-technical aspects of implementation		T1:6.1 T2:5.8
49-50-51	10-03-2020	security certification and accreditation	To study about security certification and accreditation		T1:6.2
52-53	12-03-2020	positioning and staffing security function	Recruitment of various security system developers		T1:6.3
54-55-56	13-03-2020	security management models	To study about security management models		T1:6.4
57-58	16-03-2020	credentials of information security professionals	credentials of information security professionals		T1:6.5
59-60	23-03-2020	security maintenance model, digital forensics	security maintenance model, digital forensics mechanisms		T1:6.6

IX. Mapping course outcomes leading to the achievement of the program outcomes:

Course Outcomes	Program Outcomes												
	A	**b**	**C**	**D**	**E**	**f**	**G**	**h**	**i**	**J**	**k**	**l**	**M**
1	S	H											
2			H		S								
3			H										
4				H									S
5					H								S
6					H								
7			H										
8											H		
9								H					
10								H					

S = Supportive **H = Highly Related**

Justification of Course syllabus covering Course Outcomes:

By covering the syllabus a student can understand the designing of object oriented software projects. Student is able to develop the real time projects regarding object oriented software engineering.

Justification of CO's –PO's Mapping Table:

By mapping CO-1 to the PO's A & B which are related to the course CO1: The student is able to analyze and Implement the algorithms for specific problem.

By mapping CO-2 to the PO's C & E, which are related to the course CO2: The student is able to analyze the problem and solutions using specific approach.

By mapping CO-3 to the PO's C which are related to the course CO3: The student is able to understand the purpose of different algorithms and improves the analyzing skills.

By mapping CO-4 to the PO's D & S which are related to the course CO4: The student is able to understand the Purpose of different problem oriented skills.

By mapping CO-5 to the PO's E & S which are related to the course CO5: The student is able to understand the Purpose of different reasoning skills according to their knowledge.

By mapping CO-6 to the PO's E which are related to the course CO6: The student is able to understand the concept of logical solution for given problem.

By mapping CO-7 to the PO's C which are related to the course CO7: The student is able to different conceptual and technical skills in the analysis and design.

By mapping CO-8 to the PO's K which are related to the course CO8: The student is able to understand the how to write different sorting and searching algorithms.

By mapping CO-9 to the PO's H which are related to the course CO9: The student is able to understand the purpose of why we are going for various methods for developing algorithms.

By mapping CO-10 to the PO's Hwhich are related to the course CO10: The student is able to develop fundamental algorithms as well as how to use these algorithms for implementing the logical solution for the given problem.