Course code	Course Name	L-T-P - Credits	Year of Introduction
CS472	PRINCIPLES OF INFORMATION SECURITY	3-0-0-3	2016

Course Objectives

- To introduce fundamental concepts of security.
- To introduce and discuss the relevance of security in operating system, web services etc.
- To introduce fundamental concepts of secure electronic transactions.

Syllabus

Overview of computer security, Security concepts, Need of Security, Access Control, Access control matrix, Security policies, Software vulnerabilities, Security in current domains - Wireless LAN security, Cell phone security, Secure Electronic transactions, Web Services security

Expected Outcome:

The Student will be able to :

i. appreciate the common threats faced today
ii. interpret the foundational theory behind information security
iii. design a secure system
iv. identify the potential vulnerabilities in software
v. appreciate the relevance of security in various domains
vi. develop secure web services and perform secure e-transactions

Text Books:

1. Bernard Menezes, Network security and Cryptography, Cengage Learning India, 2010.
2. M Bishop, Computer Security: Art and Science, Pearson Education, 2003.

References:

1. E Whiteman and J Mattord, Principles of information security 4th edn, Cengage Learning
2. V K Pachghare, Cryptography and information security, PHI
3. Behrousz A Forouzan, D Mukhopadhyay, Cryptography and network Security, McGraw Hill
4. W Mao, Modern Cryptography: Theory & Practice, Pearson Education, 2004.
5. C P. Fleeger and S L Fleeger, Security in Computing, 3/e, Pearson Education, 2003.

Course Plan

Module	Contents	Hours	End Sem. Exam Marks
I	**Introduction**: Overview of computer security, Security concepts, Need of Security- Threats- Deliberate software attacks, Deviation in quality of service, Attacks- malicious code, brute force, Timing attack, sniffers **Access Control Mechanisms** - Access Control, Access control matrix, Access control in OS-Discretionary and Mandatory access control, Role-based access control, case study SELinux	7	15%

II	**Security policies and models**: confidentiality policies, Bell-LaPadula model, Integrity policies, Biba model, Clark-Wilson models, Chinese wall model, waterfall model	7	15%
FIRST INTERNAL EXAMINATION			
III	**Software vulnerabilities**: Buffer and stack overflow, Cross-site scripting(XSS) , and vulnerabilities, SQL injection and vulnerabilities , Phishing.	6	15%
IV	**Malware**: Viruses, Worms and Trojans. Topological worms. Internet propagation models for worms.	6	15%
SECOND INTERNAL EXAMINATION			
V	**Security in current domains:** Wireless LAN security - WEP details. wireless LAN vulnerabilities – frame spoofing. Cellphone security - GSM and UMTS security. Mobile malware - bluetooth security issues.	8	20%
VI	**Secure Electronics transactions: F**ramework, strength and weakness, Security in current applications : Online banking , Credit Card Payment Systems. **Web Services security**: XML, SOAP, SAML, RFID	8	20%
END SEMESTER EXAM			

Question Paper Pattern (End semester exam)

1. There will be ***FOUR*** parts in the question paper – **A, B, C, D**
2. **Part A**
   a. **Total marks : 40**
   b. ***TEN*** questions, each have **4 marks**, covering **all the SIX modules** (***THREE*** questions from **modules I & II**; ***THREE*** questions from **modules III & IV**; ***FOUR*** questions from **modules V & VI**). ***All*** questions are to be answered.
3. **Part B**
   a. **Total marks : 18**
   b. ***THREE*** questions, each having **9 marks**. One question is from **module I**; one question is from **module II**; one question ***uniformly*** covers **modules I & II**.
   c. ***Any TWO*** questions have to be answered.
   d. Each question can have ***maximum THREE*** subparts.
4. **Part C**
   a. **Total marks : 18**
   b. ***THREE*** questions, each having **9 marks**. One question is from **module III**; one question is from **module IV**; one question ***uniformly*** covers **modules III & IV**.
   c. ***Any TWO*** questions have to be answered.
   d. Each question can have ***maximum THREE*** subparts.
5. **Part D**
   a. **Total marks : 24**
   b. ***THREE*** questions, each having **12 marks**. One question is from **module V**; one question is from **module VI**; one question ***uniformly*** covers **modules V & VI**.
   c. ***Any TWO*** questions have to be answered.
   d. Each question can have ***maximum THREE*** subparts.
6. There will be ***AT LEAST* 60%** analytical/numerical questions in all possible combinations of question choices.