28-11-2024 02:13:12 PM

INFORMATION SECURITY — Course Code : 314319

Programme Name/s	: **Information Technology/ Computer Science & Information Technology**
Programme Code	: **IF/ IH**
Semester	: **Fourth**
Course Title	: **INFORMATION SECURITY**
Course Code	: **314319**

I. RATIONALE

Information security protects information from unauthorized access and activities. It is important for students to be aware of security issues and technologies involved to ensure information safety and privacy. This course focuses on various techniques used to encrypt data while transferring it on network. Also includes prevention measures to protect data from security threats and attacks.

II. INDUSTRY / EMPLOYER EXPECTED OUTCOME

Implement policies and guidelines to maintain data security and privacy during data transmission.

III. COURSE LEVEL LEARNING OUTCOMES (COS)

Students will be able to achieve & demonstrate the following COs on completion of course based learning

- CO1 - Identify types of attacks which causes threat to Information Security.
- CO2 - Apply multi-factor user authentication and access control mechanisms on file, folder, device and applications.
- CO3 - Apply basic encryption / decryption techniques for a given text.
- CO4 - Apply various encryption algorithms used for information security.
- CO5 - Implement security techniques to prevent internet threats.

IV. TEACHING-LEARNING & ASSESSMENT SCHEME

Course Code	Course Title	Abbr	Course Category/s	Learning Scheme					Credits	Assessment Scheme													Total Marks
				Actual Contact Hrs./Week			SLH	NLH		Paper Duration	Theory				Based on LL & TL				Based on SL				
															Practical								
				CL	TL	LL					FA-TH	SA-TH	Total		FA-PR		SA-PR		SLA				
											Max	Max	Max	Min	Max	Min	Max	Min	Max	Min			
314319	INFORMATION SECURITY	INS	AEC	3	-	2	1	6	3	3	30	70	100	40	25	10	25@	10	25	10			175

MSBTE Approval Dt. 21/11/2024   **Semester - 4, K Scheme**

INFORMATION SECURITY   **Course Code : 314319**

Total IKS Hrs for Sem. : 0 Hrs

Abbreviations: CL- ClassRoom Learning , TL- Tutorial Learning, LL-Laboratory Learning, SLH-Self Learning Hours, NLH-Notional Learning Hours, FA - Formative Assessment, SA -Summative assessment, IKS - Indian Knowledge System, SLA - Self Learning Assessment

Legends: @ Internal Assessment, # External Assessment, *# On Line Examination , @$ Internal Online Examination

Note :

1. FA-TH represents average of two class tests of 30 marks each conducted during the semester.
2. If candidate is not securing minimum passing marks in FA-PR of any course then the candidate shall be declared as "Detained" in that semester.
3. If candidate is not securing minimum passing marks in SLA of any course then the candidate shall be declared as fail and will have to repeat and resubmit SLA work.
4. Notional Learning hours for the semester are (CL+LL+TL+SL)hrs.* 15 Weeks
5. 1 credit is equivalent to 30 Notional hrs.
6. * Self learning hours shall not be reflected in the Time Table.
7. * Self learning includes micro project / assignment / other activities.

V. THEORY LEARNING OUTCOMES AND ALIGNED COURSE CONTENT

Sr.No	Theory Learning Outcomes (TLO's)aligned to CO's.	Learning content mapped with Theory Learning Outcomes (TLO's) and CO's.	Suggested Learning Pedagogies.
1	TLO 1.1 Explain Need of information security. TLO 1.2 State criteria for information classification. TLO 1.3 Explain basic principles of information security. TLO 1.4 Identify various types of attacks. TLO 1.5 Enlist types of malware. TLO 1.6 Establish relationship between threat, vulnerability, risks with suitable example.	**Unit - I Introduction to Information Security** 1.1 Information Security Overview: Introduction to information, need of information security 1.2 Information classification, Criteria for information classification 1.3 Basic principles of information security: Confidentiality, Authentication, Integrity, Availability, Access Controls, Repudiation 1.4 Type of Attacks: Active and Passive attacks, Denial of Service, DDOS, Backdoors and Trapdoors, Sniffing, phishing, Spoofing, Man in the Middle, Replay, TCP/IP Hacking, Encryption attacks, Social Engineering 1.5 Types of Malwares and their impact on security and prevention: - Virus, Worms, Trojan horse, Spyware, Adware, Ransomware, Logic Bombs, Rootkits, Backdoors, Keyloggers 1.6 Threat and Risk Analysis: Introduction to assets, vulnerability, threats, risks, relation between: threat, vulnerability, risks	Lecture Using Chalk-Board Presentations Video Demonstrations

MSBTE Approval Dt. 21/11/2024   **Semester - 4, K Scheme**

INFORMATION SECURITY   **Course Code : 314319**

Sr.No	Theory Learning Outcomes (TLO's)aligned to CO's.	Learning content mapped with Theory Learning Outcomes (TLO's) and CO's.	Suggested Learning Pedagogies.
2	TLO 2.1 Use different types of authentication methods. TLO 2.2 Identify various types of password attacks. TLO 2.3 Illustrate the given biometric patterns. TLO 2.4 State goals of authorization. TLO 2.5 Compare DAC, MAC, RBAC and ABAC on the basis of given parameters.	**Unit - II User Authentication and Access Control** 2.1 Identification and Authentication methods : Electronic user authentication, username and password, multi-factor authentication, token-based authentication, biometrics 2.2 Guessing password, Password attacks : Piggybacking, Shoulder surfing, Dumpster diving 2.3 Biometrics : Finger prints, Hand prints, Retina scan patterns, Voice patterns 2.4 Authorization : Introduction to authorization, goals of authorization 2.5 Access controls : Access control principles, Access rights and permission Access control policies : Discretionary access control (DAC), Mandatory access control (MAC), Role-based access control (RBAC), Attribute-based access control (ABAC)	Lecture Using Chalk-Board Presentations Video Demonstrations
3	TLO 3.1 Explain the process of encryption and decryption. TLO 3.2 Compare symmetric and asymmetric cryptography on the basis of given parameters. TLO 3.3 Apply given substitution techniques on text. TLO 3.4 Apply given transposition techniques on text. TLO 3.5 Explain step by step working of steganography.	**Unit - III Fundamentals of Cryptography** 3.1 Introduction : Plain text, Cipher text, Cryptography, Cryptanalysis, Cryptology, Encryption, Decryption 3.2 Symmetric and Asymmetric cryptography : Introduction, working, key management, asymmetric cryptography -public key distribution 3.3 Substitution techniques : Caesar cipher, Playfair cipher, Vigenere cipher, Vernam cipher (One-time pad) 3.4 Transposition techniques : Rail fence technique , Simple columnar technique 3.5 Steganography : Introduction and working of steganography	Lecture Using Chalk-Board Presentations Video Demonstrations
4	TLO 4.1 Apply DES algorithm to encrypt given text. TLO 4.2 Apply AES algorithm to encrypt given text. TLO 4.3 Apply given algorithm to perform encryption on text. TLO 4.4 Apply hash function algorithm to generate hash value for given text. TLO 4.5 Explain working of Digital Signature. TLO 4.6 Enlist mobile security threats.	**Unit - IV Encryption Algorithms** 4.1 DES (Data Encryption Standard) algorithm 4.2 AES (Advanced Encryption Standard) algorithm 4.3 RSA algorithm 4.4 Diffie-Hellman key exchange algorithm, Man-in-middle attack 4.5 Hash Function : Introduction, Features of Hash Functions, MD5 and SHA algorithm 4.6 Digital Signature : Introduction and working of digital signature 4.7 Threats to mobile phone and its security measures	Lecture Using Chalk-Board Presentations Video Demonstrations Flipped Classroom

MSBTE Approval Dt. 21/11/2024   **Semester - 4, K Scheme**

INFORMATION SECURITY   **Course Code : 314319**

Sr.No	Theory Learning Outcomes (TLO's)aligned to CO's.	Learning content mapped with Theory Learning Outcomes (TLO's) and CO's.	Suggested Learning Pedagogies.
5	TLO 5.1 Explain given type of firewalls. TLO 5.2 Enlist firewall policies. TLO 5.3 Compare Network Based and Host-Based IDS. TLO 5.4 Explain given protocol used for E-mail security. TLO 5.5 Identify type of cyber-crime for a given scenario. TLO 5.6 Explain categories of cyber laws.	**Unit - V Internet Security and Cyber Law** 5.1 Firewall : Need of firewall, Types of firewalls : Packet filters, Stateful packet filters, Application gateways, Circuit gateways 5.2 Firewall policies, Configuration, Limitations, Demilitarized zone (DMZ) 5.3 Intrusion Detection System(IDS) : Network-based IDS, Host-based IDS, Honeypots 5.4 E-mail security : Simple mail transfer protocol (SMTP), Pretty good privacy (PGP), S/MIME 5.5 Cyber crime: Introduction, Hacking, Digital forgery, Cyber stalking/Harassment, Cyber pornography, Identity theft & fraud, Cyber terrorism, Cyber defamation, OS fingerprinting 5.6 Cyber Laws: Introduction, Need, Categories: Crime against individual, Government, Property	Lecture Using Chalk-Board Presentations Video Demonstrations Case Study Site/Industry Visit

VI. LABORATORY LEARNING OUTCOME AND ALIGNED PRACTICAL / TUTORIAL EXPERIENCES.

Practical / Tutorial / Laboratory Learning Outcome (LLO)	Sr No	Laboratory Experiment / Practical Titles / Tutorial Titles	Number of hrs.	Relevant COs
LLO 1.1 Install and configure Antivirus software on system. LLO 1.2 Apply privacy and security settings to protect operating system.	1	*i. Install and configure Antivirus software on system (Licensed copy) ii. Use privacy and security settings on operating system	2	CO1
LLO 2.1 Set up and recover password of computer system.	2	*i.Set up single level authentication for computer system ii.Recover the password of computer system using any freeware password recovery tool (Example- John the ripper)	2	CO2
LLO 3.1 Grant read , write and execute permission on file and folder.	3	*i.Grant security to file, folder or application using access permissions and verify it ii.Grant access permission while sharing file and folder	2	CO2
LLO 4.1 Implement password authentication.	4	Write a utility using C/Shell programming to create strong password authentication (Password should be more than 8 characters, and combination of digits, letters and special characters #, %, &, @)	2	CO2
LLO 5.1 Implement caesar cipher encryption technique.	5	*i.Write a C program to implement caesar cipher technique to perform encryption and decryption of text ii.Apply Caesar cipher technique to perform encryption and decryption of text using any open-source tool (Example - Cryptool)	2	CO3

MSBTE Approval Dt. 21/11/2024   **Semester - 4, K Scheme**

INFORMATION SECURITY   **Course Code : 314319**

Practical / Tutorial / Laboratory Learning Outcome (LLO)	Sr No	Laboratory Experiment / Practical Titles / Tutorial Titles	Number of hrs.	Relevant COs
LLO 6.1 Implement Vernam cipher encryption technique.	6	i.Implement Vernam cipher encryption technique to perform encryption of text using C programming language ii.Apply Vernam cipher technique to perform encryption and decryption of text using any open-source tool (Example - Cryptool)	2	CO3
LLO 7.1 Implement rail fence encryption technique.	7	* Implement rail fence encryption technique to perform encryption of text using C programming language	2	CO3
LLO 8.1 Implement simple columnar transposition technique.	8	Implement simple Columnar Transposition encryption technique to perform encryption of text using C programming language	2	CO3
LLO 9.1 Generate Hash Code.	9	Create and verify Hash Code for given message using any Open-source tool. (Example-Cryptool)	2	CO3
LLO 10.1 Implement Diffie-Hellman key exchange encryption technique.	10	i.Write a C program to implement Diffie-Hellman key exchange algorithm to perform encryption of text ii.Use Diffie-Hellman key exchange algorithm to perform encryption and decryption of text using any open-source tool (Example - Cryptool)	2	CO4
LLO 11.1 Implement steganography.	11	* Use Steganography to encode and decode the message using any open-source tool (Example-OpenStego)	2	CO4
LLO 12.1 Generate digital signature.	12	* Create and verify digital signature using any Open-source tool (Example-Cryptool)	2	CO4
LLO 13.1 Configure firewall.	13	* Configure firewall settings on any operating system	2	CO5
LLO 14.1 Implement email security.	14	Send a test mail securely using any open-source tool (Example- Pretty Good Privacy with GnuPG)	2	CO5
LLO 15.1 Apply browser settings.	15	Set up security policies for any web browser and Email account (Example: setting filter, spam for email security. Low security apps settings, cookies, synchronization for web browser))	2	CO1 CO5

Note : Out of above suggestive LLOs -

- '*' Marked Practicals (LLOs) Are mandatory.
- Minimum 80% of above list of lab experiment are to be performed.
- Judicial mix of LLOs are to be performed to achieve desired outcomes.

VII.   SUGGESTED MICRO PROJECT / ASSIGNMENT/ ACTIVITIES FOR SPECIFIC LEARNING / SKILLS DEVELOPMENT (SELF LEARNING)

Micro project

- User A wants to send message to user B securely on network.
i. Select any two techniques to encrypt message.
ii. Implement both the techniques.
iii. Evaluate result of implementation.
iv. Compare complexity of both techniques.
v. Prepare report.

MSBTE Approval Dt. 21/11/2024   **Semester - 4, K Scheme**

INFORMATION SECURITY	**Course Code : 314319**

- Prepare admin level report of company who wants to implement allocate fixed system to each employee for authentic access to maintain security.

i. Explain various single level authentication method available to access the system.

ii. Analyse the weakness and security threats to this problem.

iii. Suggest multi factor authentication for given problem situation.

iv. Compare impact of single and multi-factor authentication on given situation.

- A bank has more than 1000 user accounts. Around 100 users received message regarding deduction of specific amount without intimation and after that all authorized user are not able to access online banking service of that bank.

i. Identify type of crime and attack.

ii. Write procedure to investigate that crime.

iii. Write preventive measure to avoid such type of attack in future.

iv. Write punishment of such type of attacks and state cyber law act.

v. Write a report.

- Case study on Cyber Crime in Social Engineering in India.

i. Explain various Social Engineering attacks.

ii. Select topic for case study.

iii. Write problem statement of attack.

iv. Write procedure to investigate that attack.

v. Write a report.

- Teacher shall allocate any other microproject relevant to COs.

Assignment

- Teacher shall give assignments covering all COs.

Other

- Complete any one course related to Information Security and Cyber Crime on Infosys Springboard , Virtual Lab , NPTEL.

Note :

- Above is just a suggestive list of microprojects and assignments; faculty must prepare their own bank of microprojects, assignments, and activities in a similar way.
- The faculty must allocate judicial mix of tasks, considering the weaknesses and / strengths of the student in acquiring the desired skills.
- If a microproject is assigned, it is expected to be completed as a group activity.
- SLA marks shall be awarded as per the continuous assessment record.
- For courses with no SLA component the list of suggestive microprojects / assignments/ activities are optional, faculty may encourage students to perform these tasks for enhanced learning experiences.
- If the course does not have associated SLA component, above suggestive listings is applicable to Tutorials and maybe considered for FA-PR evaluations.

VIII. LABORATORY EQUIPMENT / INSTRUMENTS / TOOLS / SOFTWARE REQUIRED

Sr.No	Equipment Name with Broad Specifications	Relevant LLO Number
1	Steganography Tools. (Open-source tool)	11
2	E-mail Security Tool. (Open-source tool)	14
3	Web Browser. (Any Web Browser)	15
4	Any freeware password recovery tool.	2
5	Any compiler (TurboC / Online 'C' compiler)	4,5,6,7,8,10

MSBTE Approval Dt. 21/11/2024   **Semester - 4, K Scheme**

INFORMATION SECURITY		**Course Code : 314319**

Sr.No	Equipment Name with Broad Specifications	Relevant LLO Number
6	Encryption and decryption tool. (Open-source tool)	5,6,9,10,12
7	Antivirus software (Licensed copy)	All
8	Computer System (Any computer system with basic configuration)	All

IX. SUGGESTED WEIGHTAGE TO LEARNING EFFORTS & ASSESSMENT PURPOSE (Specification Table)

Sr.No	Unit	Unit Title	Aligned COs	Learning Hours	R-Level	U-Level	A-Level	Total Marks
1	I	Introduction to Information Security	CO1	9	4	6	2	12
2	II	User Authentication and Access Control	CO2	8	4	4	4	12
3	III	Fundamentals of Cryptography	CO3	10	2	4	10	16
4	IV	Encryption Algorithms	CO4	8	2	4	8	14
5	V	Internet Security and Cyber Law	CO5	10	6	6	4	16
		Grand Total		**45**	**18**	**24**	**28**	**70**

X. ASSESSMENT METHODOLOGIES/TOOLS

Formative assessment (Assessment for Learning)

• Continuous assessment based on process and product related performance indicators
Each practical will be assessed considering
   60% weightage to process
   40% weightage to product
A continuous assessment based on term work

Summative Assessment (Assessment of Learning)

• End semester examination, Lab performance, Viva voce

XI. SUGGESTED COS - POS MATRIX FORM

Course Outcomes (COs)	Programme Outcomes (POs)							Programme Specific Outcomes* (PSOs)		
	PO-1 Basic and Discipline Specific Knowledge	PO-2 Problem Analysis	PO-3 Design/ Development of Solutions	PO-4 Engineering Tools	PO-5 Engineering Practices for Society, Sustainability and Environment	PO-6 Project Management	PO-7 Life Long Learning	PSO-1	PSO-2	PSO-3
CO1	2	-	-	-	1	1	2			
CO2	1	1	1	1	2	2	2			
CO3	1	2	2	2	2	1	2			
CO4	1	2	2	2	2	1	2			

MSBTE Approval Dt. 21/11/2024   **Semester - 4, K Scheme**

INFORMATION SECURITY   **Course Code : 314319**

CO5	1	1	1	2	2	1	3			

Legends :- High:03, Medium:02,Low:01, No Mapping: -
*PSOs are to be formulated at institute level

XII. SUGGESTED LEARNING MATERIALS / BOOKS

Sr.No	Author	Title	Publisher with ISBN Number
1	Mark Merkow, Jim Breithaupt	Information Security Principles and Practices	Pearson. ISBN 978-81-317-1288-7
2	V. K. Pachghare	Cryptography and Information Security	Prentice Hall India ISBN:978-81-203-5082-3
3	Atul Kahate	Cryptography and Network security Third Edition	McGraw-Hill; Fourth edition ISBN-13: 978-9353163303
4	William Stallings, Lawrie Brown	Computer Security Principles and Practice, Third Edition	Pearson. ISBN-13: 978-0-13-377392-7
5	Nina Godbole	Information Systems Security Second Edition	John Wiley ISBN-13: 978-8126564057
6	Harish Chander	Cyber Laws and IT Protection Second Edition	PHI Publication , ISBN : 9789391818463 eBook ISBN : 9789391818517

XIII . LEARNING WEBSITES & PORTALS

Sr.No	Link / Portal	Description
1	https://www.youtube.com/watch?v=NlpnJE0m-NU	Simulation of Intrusion Detection System in MANET using NetSim
2	https://archive.nptel.ac.in/courses/106/106/106106129/	NPTEL course on Introduction to Information Security
3	https://onlinecourses.swayam2.ac.in/cec22_cs15/preview	Swayam course on Information Technology
4	https://www.youtube.com/watch?v=T9c5ZpT2FV0	Firewall configuration
5	https://cse29-iiith.vlabs.ac.in/List%20of%20experiments.html	Virtual lab for cryptography

Note :

- Teachers are requested to check the creative common license status/financial implications of the suggested online educational resources before use by the students

MSBTE Approval Dt. 21/11/2024   **Semester - 4, K Scheme**