|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Course Code:**  SWE3003 | **Course Title: Information and System Security** | **TPC** | **3** | **2** | **4** |
| **Version No.** | **1.0** | | | | |
| **Course Pre-requisites/ Co-requisites** | **None** | | | | |
| **Anti-requisites (if any).** | **CSE1007** | | | | |
| **Objectives:** | Objectives:   1. To learn principles of Information and System security. 2. To introduce the practices of cryptography and program security technology along with their practical use and applications. | | | | |
| **Expected Outcome:** | On completion of the course, students will have the ability to   1. Explain the basic concepts of information and systems security and the risks faced by computer systems. 2. Identify and analyze security problems in information systems. 3. Understand the principles of cryptography, network and information security and apply it in suitable security application. 4. Explain how security mechanism in computer systems work | | | | |
| **Module No. 1** | **Fundamentals of Security** | | **8 Hours** | | |
| Security attacks, methods of defence, security functional requirements, information and network security policies, Identification and Authentication Essentials, Access Control and Access control Structures, Security Models and Confidentiality, Elementary Cryptography. | | | | | |
| **Module No. 2** | **Elementary Cryptography** | | **7 Hours** | | |
| Cryptography & cryptanalysis. Classical encryption techniques, substitution techniques, transposition techniques. Block ciphers, DES, AES structure. | | | | | |
| **Module No. 3** | **Public Key Crypto Systems** | | **8 Hours** | | |
| Number theory fundamentals, principles of pubic key crypto systems, RSA algorithm, Diffie-Hellman key exchange. | | | | | |
| **Module No. 4** | **Data Base Security** | | **7 Hours** | | |
| Relational databases, Security requirements, Reliability and Integrity, Sensitive data, Inference, Multilevel secure databases, concurrency control and multilevel security, Data mining, Privacy preserving data mining | | | | | |
| **Module No. 5** | **Network Security** | | **8 Hours** | | |
| Threats in Networks, TCP/IP security, Network Security Controls, Intrusion Detection Systems, Firewalls and Intrusion Prevention Systems, Email security, Network attacks and DNS protection, Internet security procedures, Application and Data Hacking. | | | | | |
| **Module No.6** | **Program Security** | | **7 Hours** | | |
| Secure programs, Non‐malicious program errors, types of malicious software, viruses and counter measures, Bots, Rootkits, Targeted malicious code, Controls against program threats, software security issues. | | | | | |
| **Text Books**   1. William Stallings, Cryptography & Network Security- Principles and Practices, 7th Edition by Pearson Publishers, 2017. | | | | | |
| **References**   1. Charles P. Fleeger, Security in computing, 5th Edition, Pearson, 2015 | | | | | |
| **Sample Problems for Worksheets**   * 1. Encrypt the following message using Play fair mechanism.      1. Plain text: **Information System security at VIT university**      2. Keyword: **UNIVERS**   2. In how many ways we can perform authentication. Give brief explanation for each model.   3. Describe the classification of security attacks.   4. Explain in detail Military security policy and show how access control is obtained using Bell-La Padula Confidentiality Model.      1. In a public key system using RSA, you intercept the cipher text C = 10 sent to user whose public key is e= 5, n=35. Find the plaint text M?      2. Perform encryption and decryption using RSA algorithm for the following:         1. p=3, q=11, e=7, M=5         2. n=77, e=17, M=8   5. Define various modules used for implementing Access Control with their advantages and disadvantages.   6. Write a short note on      1. Types of malicious code      2. How virus works   7. Given the security levels TOPSECRET, SECRET, CONFIDENTIAL, and UNCLASSIFIED (ordered from highest to lowest), and the compartments A, B, and C, say what type of access (read, write) is allowed according to the Bell-La Padula model in the following situations and give the reason. (2.5)      1. 1. Ram, cleared for (TOPSECRET, A, C), wants to access a document classiﬁed (SECRET, A).      2. 2. Kumar, cleared for (CONFIDENTIAL, C), wants to access a document classiﬁed (CONFIDENTIAL, B ).      3. 3. Anita, cleared for (CONFIDENTIAL, C), wants to access a document classiﬁed (SECRET, C ).      4. 4. Sam, cleared for (TOPSECRET, A, C ), wants to access a document classiﬁed (CONFIDENTIAL, A ).      5. 5. Singh, who has no clearances (and so works at the UNCLASSIFIED level), wants to access a document classiﬁed (CONFIDENTIAL, B).   8. Consider the following matrix as the key and encrypt ‘CAT’ and ‘ACT’. Write your observation. Description: \begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix}   9. Apply PlayFair Cipher to decrypt the following ciphertext. The Keyword used is “MONARCHY”. UGRMKCSXHMUFMKBZ   **Practical Assessment (1 Credit)**  The world’s most comprehensive vulnerability databases, currently consisting of more than 60,000 recorded vulnerabilities (spanning more than two decades) from over 19,000 vendors representing over 54,000 products. The result is the annual Symantec Internet Security Threat Report, which gives enterprises, small businesses, and consumers essential information to secure their systems effectively now and into the future. Symantec has established the most comprehensive source of Internet threat data in the world through the Symantec™ .Global Intelligence Network, which is made up of more than 41.5 million attack sensors and records thousands of events per second. This network monitors threat activity in over 157 countries and territories through a combination of Symantec products and services such as Symantec DeepSight™.Threat Management System, Symantec™ Managed Security Services, Norton™ consumer products, and other third-party data sources.    Students can do any of the below mentioned topics:   1. Each of you take one organization and find out areas that deserve special attention. 2. The most important trends and attacks found in recent years. 3. Targeted Attacks Grow and Evolve 4. Vulnerabilities and Unpatched Websites 5. Social Media scams and malware flourish on mobile 6. Password system analysis 7. Web-security vulnerability analysis   Alternative projects require instructor's approval | | | | | |
| **Mode of Evaluation** | **Continuous Assessment Tests-60%, Practical Assessment-40%**    Continuous Assessment Test-1 20%  Continuous Assessment Test-2 20%  Continuous Assessment Test-3 20%  Practical Assessment 40% | | | | |
| **Recommended by the Board of Studies on** | 06.07.2018 | | | | |
| **Date of Approval by the Academic Council** | 2nd Academic Council 21.07.2018 | | | | |