## Government of Karnataka
## Department of Technical Education
## Bengaluru

| | | | |
|---|---|---|---|
| | **Course Title: Network Security & Management** | | |
| | Scheme (L:T:P) : **4:0:0** | Total Contact Hours: **52** | Course Code: **15CS62T** |
| | Type of Course: **Lectures, Self Study & Student Activity.** | Credit **:04** | Core/ Elective: **Core** |
| CIE- 25 Marks | | | SEE- 100 Marks |

### Prerequisites:

Knowledge of Computer Networks.

### Course Objectives

To study the concepts of network security and various cryptographic algorithms, hardware and software security, IDS, wireless security, web security, security laws with Internet Governance & Email policy.

### Course Outcome

***On successful completion of the course, the students will be able to attain below Course Outcome (CO):***

| **Course outcome** | | **CL** | **Linked PO** | **Teaching Hours** |
|---|---|---|---|---|
| **CO1** | Discuss the basic concepts of network security and various cryptographic algorithms. | ***R,U,A*** | **1,2,3,7,8,9,10** | **06** |
| **CO2** | Describe various hardware and software securities for information. | ***R,U,A*** | **1,2,3,7,8,9,10** | **14** |
| **CO3** | Discuss how Intrusion Detection System helps to provide security along with various types of firewalls. | ***R,U,A*** | **1,2,3,7,8,9,10** | **06** |
| **CO4** | Describe how wireless security provided to information. | ***R,U*** | **1,2,3,7,8,9,10** | **06** |
| **CO5** | Discuss various concepts of web security. | ***R,U*** | **1,2,3,7,8,9,10** | **12** |
| **CO6** | Discuss security and law along with Internet Governance and Email policy. | ***R,U*** | **1,2,3,7,8,9,10** | **08** |
| | | | **Total** | **52** |

**Legends:** R = Remember U= Understand; A= Apply and above levels (Bloom's revised taxonomy)

### Course-PO Attainment Matrix

| Course | Programme Outcomes | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| **Network Security & Management** | **3** | **3** | **3** | **-** | **-** | **-** | **3** | **3** | **3** | **3** |

**Level 3- Highly Addressed, Level 2-Moderately Addressed, Level 1-Low Addressed.**

Method is to relate the level of PO with the number of hours devoted to the COs which address the given PO.
If ≥40% of classroom sessions addressing a particular PO, it is considered that PO is addressed at Level 3
If 25 to 40% of classroom sessions addressing a particular PO, it is considered that PO is addressed at Level 2
If 5 to 25% of classroom sessions addressing a particular PO, it is considered that PO is addressed at Level 1
If < 5% of classroom sessions addressing a particular PO, it is considered that PO is considered not-addressed.

## Course Content and Blue Print of Marks for SEE

| Unit No | Unit Name | Hour | Questions to be set for SEE | | | Marks Weightage | Marks Weightage (%) |
|---|---|---|---|---|---|---|---|
| | | | R | U | A | A | |
| I | Introduction and Cryptography | **16** | 10 | 10 | 20 | 40 | 27.58 |
| II | Hardware & Software Security | **06** | 05 | 05 | 05 | 15 | 10.34 |
| III | Intrusion Detection System and Firewalls | **10** | 10 | 10 | 10 | 30 | 20.68 |
| IV | Wireless Security | **06** | 05 | 15 | - | 20 | 13.79 |
| V | Web Security | **08** | 05 | 20 | - | 25 | 17.24 |
| VI | Security and Law, Internet Governance and Email Policy | **06** | 05 | 10 | - | 15 | 13.79 |
| | **Total** | **52** | **40** | **70** | **35** | **145** | **100** |

## UNIT I : Introduction and Cryptography 16 Hrs

**Introduction:** Computer security concepts, The OSI security architecture, Security attacks, Security services, Security mechanisms, A model for network security, Standards

**Cryptography:** Symmetric Encryption Principles, Symmetric Block Encryption Algorithms, Random and Pseudorandom Numbers, Stream Ciphers and RC4, Cipher Block Modes of Operation, Approaches to Message Authentication, Secure Hash Function, Message Authentication Codes, Public Key Cryptography Principles, Public-Key Cryptography Algorithms, Digital Signatures.

## UNIT II: Hardware and Software Security 06 Hrs

Hardware Security, Smart Cards, Biometrics, Virtual Private Networks, Types of VPN's, Trusted Operating Systems, Pretty Good Privacy (PGP), Security Protocols, Security Socket Layer, Transport Layer Security, IPSec, S/MIME(Secure/Multipurpose Internet Mail Extension)

## UNIT III: Intrusion Detection System and Firewalls 10 Hrs

**IDS:** What is not an IDS?, Infrastructure of IDS, Classification of IDS, Host-based IDS, Network based IDS, Anomaly Vs Signature Detection, Normal Behaviour Patterns-Anomaly Detection, Misbehaviour Signatures-Signature Detection , Parameter Pattern Matching, Manage an IDS.

Malicious Software, Safeguards, Firewalls, Packet-Filtering Firewalls, State full Inspection Firewalls, Proxy firewalls, Guard, Personal Firewalls, Limitations of Firewalls.

## UNIT IV: Wireless Security 06 Hrs

Wireless Application Protocol, WAP Security, Authentication, Integrity, Confidentiality, Security Issues with Wireless Transport Layer Security (WTLS), Wireless LAN, WLAN Configuration, WLAN Technology consideration, Wireless LAN Security, Access Point Security, Work Station Security, Safeguarding Wireless LAN's.

## UNIT V: Web Security 08 Hrs

Client/Server Architecture, Security considerations and Threats, Web traffic security approaches, SSL/TLS for secure web services, The Twin concept of "SSL Connection" and "SSL Session", SSL session state, SSL Connection State, SSL Record Protocol, SSL Handshake Protocol, Secure Hypertext Transport Protocol(S-HTTP), Secure Electronic Transaction(SET), Business Requirements, SET Participants, SET Transaction Flow.

## UNIT VI: Security and Law, Internet Governance and Email Policy 06 Hrs

**Security and Law:** Regulations in India, Information Technology Act 2000, Cyber Crime and the IT Act 2000, Indian Contract Act, 1872, Indian Penal Code, Indian Copyright Act, Consumer Protection Act, 1986, Specific Relief Act, 1963, Government Initiatives, Future Trends-Law of Convergence.

**Internet Governance and Email Policy:** Internet Governance, Network Security Aspects in E-Governance, Security Monitoring Tools, Electronic Mail, What are the e-mail Threats that Organization's face?, Why do you need an E-mail Policy?, How do you create an E-mail Policy?, Publishing the E-mail Policy, University E-mail Policy, Electronic mail policy.

## Text books

1. **Network Security Essentials: Applications and Standards**, 4/e, William Stallings, Pearson Educaiton, ISBN: 9788131716649 (Chap 1)
2. **Network Security and Management**, 2nd edition, Brijendra Sing, PHI, ISBN: 9788120339101 (Chap: 2,3,4,5,6)

## References

1. Network Security Bible, 2nd edition, Eric Cole, Wiley Publisher, ISBN: 9788126523313

## Suggested list of student activities

***Note: the following activities or similar activities for assessing CIE (IA) for 5 marks (Any one)***

1. Each individual student should do any one of the following type activity or any other similar activity related to the course and before conduction, get it approved from concerned course coordinator and programme coordinator.
2. Each student should conduct different activity and no repetition should occur.

| | |
|---|---|
| 1 | Make a survey in any industry/ institute to understand the way security is provided for information. Videos can also be used to make the survey. |
| 2 | Quiz |

## Course Delivery

The course will be delivered through lectures and Power point presentations/ Video

## Course Assessment and Evaluation Scheme

| Method | What | | To whom | When/Where (Frequency in the course) | Max Marks | Evidence collected | Course outcomes |
|---|---|---|---|---|---|---|---|
| Direct Assessment | CIE | IA | Students | Three IA tests (Average of three tests will be computed) | 20 | Blue books | 1 to 6 |
| | | | | Student activities | 05 | Report | 1 to 6 |
| | | | | **Total** | **25** | | |
| | SEE | End Exam | | **End of the course** | **100** | Answer scripts at BTE | 1 to 6 |
| Indirect Assessment | | | Students | Middle of the course | | Feedback forms | 1, 2, 3 Delivery of course |
| | End of Course Survey | | | End of the course | | Questionnaires | 1 to 6 Effectiveness of Delivery of instructions & Assessment Methods |

**Note:** I.A. test shall be conducted for 20 marks. Average marks of three tests shall be rounded off to the next higher digit.

**Questions for CIE and SEE will be designed to evaluate the various educational components (Bloom's taxonomy) such as:**

| Sl. No | Bloom's Category | % |
|---|---|---|
| 1 | Remembrance | 28 |
| 2 | Understanding | 48 |
| 3 | Application | 24 |

***Note to IA verifier**: The following documents to be verified by CIE verifier at the end of semester*

1. Blue books (20 marks)
2. Student suggested activities report for 5 marks

3. Student feedback on course regarding Effectiveness of Delivery of instructions & Assessment Methods.

## FORMAT OF I A TEST QUESTION PAPER (CIE)

| Test/Date and Time | Semester/year | Course/Course Code | Max Marks |
|---|---|---|---|
| Ex: I test/6 th week of sem 10-11 AM | VI SEM | | 20 |
| | Year: 2017-18 | | |

Name of Course coordinator :
Units:__ CO's:____

| Question no | Question | MARKS | CL | CO | PO |
|---|---|---|---|---|---|
| 1 | | | | | |
| 2 | | | | | |
| 3 | | | | | |
| 4 | | | | | |

**Note: Internal choice may be given in each CO at the same cognitive level (CL).**

## MODEL QUESTION PAPER (CIE)

| Test/Date and Time | Semester/year | Course/Course Code | Max Marks |
|---|---|---|---|
| Ex: I test/6 th week of sem 10-11 AM | VI SEM | Network Security Management | 20 |
| | Year: 2017-18 | Course code: **15CS62T** | |

Name of Course coordinator :
Units:1,2 Co: 1,2

**Note: Answer all questions**

| Question no | Question | CL | CO | PO |
|---|---|---|---|---|
| 1 | List the differences between passive and active security threats.(5) OR List out the design objectives for HMAC.(5) | R | 1 | 1,2 |
| 2 | Explain essential ingredients of a symmetric cipher with a neat diagram (5) OR Describe the advantages of counter mode. (5) | U | 1 | 1,2 |
| 3 | Explain with a neat diagram Fiestel Cipher Structure and its design elements.(10) | A | 1 | 1,2 |

## Format for Student Activity Assessment

| DIMENSION | Unsatisfactory 1 | Developing 2 | Satisfactory 3 | Good 4 | Exemplary 5 | Score |
|---|---|---|---|---|---|---|
| **Collection of data** | Does not collect any information relating to the topic | Collects very limited information; some relate to the topic | Collects some basic information; refer to the topic | Collects relevant information; concerned to the topic | Collects a great deal of information; all refer to the topic | 3 |
| **Fulfill team's roles & duties** | Does not perform any duties assigned to the team role | Performs very little duties | Performs nearly all duties | Performs all duties | Performs all duties of assigned team roles with presentation | 4 |
| **Shares work equally** | Always relies on others to do the work | Rarely does the assigned work; often needs reminding | Usually does the assigned work; rarely needs reminding | Does the assigned job without having to be reminded. | Always does the assigned work without having to be reminded and on given time frame | 3 |
| **Listen to other Team mates** | Is always talking; never allows anyone else to speak | Usually does most of the talking; rarely allows others to speak | Listens, but sometimes talk too much | Listens and contributes to the relevant topic | Listens and contributes precisely to the relevant topic and exhibit leadership qualities | 3 |
| | | | | | **TOTAL** | **13/4=3.25=4** |

**Note: This is only an example. Appropriate rubrics/criteria may be devised by the concerned Course Coordinator for assessing the given activity**

**MODEL QUESTION PAPER** Code: **15CS62T**

**Diploma in Computer Science & Engineering**

**VI- Semester**

**Course Title: Network Security & Management**

Time: **3 Hours** Max Marks**: 100**

## PART-A

**Answer any SIX questions. Each carries 5 marks. 5X6=30 Marks**

1. List the differences between passive and active security threats.
2. Explain essential ingredients of a symmetric cipher with a neat diagram
3. List out the design objectives for HMAC.
4. Describe the advantages of counter mode.
5. Write a note on S/MIME.
6. Describe the classification of IDS.
7. Mention the purpose of firewalls and its limitations.
8. Explain how to safeguard Wireless LANs.
9. List the services provided by SSL record protocol.
10. Write a short note on Indian Penal Code.

## PART-B

**Answer any SEVEN full questions each carries 10 marks. 10X7=70 Marks**

1. Explain in detail various security services.
2. Explain with a neat diagram Fiestel Cipher Structure and its design elements.
3. Explain the RSA public-key Encryption algorithm with an example.
4. Explain the various hardware securities ( Smartcard and Biometrics ).
5. Write a note on network based IDS.
6. Explain Packet Filtering Firewall and its importance.
7. Describe WAP protocol architecture.
8. Describe the SET components and their relationships.
9. Explain how do you create an email policy for your organization.

## MODEL QUESTION BANK

**Diploma in Computer Science & Engineering**

**VI Semester**

**Course Title: Network Security & Management**

| CO | Question | CL | Marks |
|---|---|---|---|

|  |  |  |  |
|---|---|---|---|
| I | Explain OSI security architecture. | U | 05 |
|  | List the differences between passive and active security threats. | R |  |
|  | Define categories of passive and active passive attacks. | R |  |
|  | Define categories of security services. | R |  |
|  | Discuss categories of security mechanisms. | U |  |
|  | Write three key objectives of computer security. | U |  |
|  | Explain essential ingredients of a symmetric cipher with a neat diagram. | U |  |
|  | Describe cryptography, cryptanalysis and various types of attacks on it. | U |  |
|  | Explain CBC mode operations with neat diagram. | U |  |
|  | Explain CTR mode operation with neat diagram. | U |  |
|  | Explain message authentication code with a neat diagram | U |  |
|  | List the design objectives of HMAC. | U |  |
|  | Describe the advantages of counter mode. | U |  |
|  | Explain in detail various security services. | U | 10 |
|  | Explain network security model with a neat diagram. | U |  |
|  | Explain with a neat diagram Feistel Cipher Structure and its design elements. | A |  |
|  | Explain AES algorithm with a neat diagram. | A |  |
|  | Describe Data Encryption Standard with a neat diagram | A |  |
|  | Explain with a neat diagram Stream Cipher Structure and list its important design considerations. | A |  |
|  | Describe RC4 algorithm with a neat diagram. | A |  |
|  | Explain the RSA public-key Encryption algorithm with an example. | A |  |
|  | Explain message authentication using one way hash function with a neat diagram. | A |  |
|  | Write public key encryption structure with neat diagram. | A |  |
|  | Perform Encryption and Decryption using RSA algorithm for the following values<br>P=3,q=11,e=7,M=5 | A |  |
|  | In a RSA system the Public Key of a given user is e=31,n=3599 what is the private key of this user? | A |  |
| II | Describe trusted operating system. | R | 05 |
|  | Explain hardware security. Give an example of common hardware problem and safeguards for hardware security. | U |  |
|  | Explain Pretty Good Privacy (PGP). | U |  |
|  | Write a note on S/MIME. | U |  |
|  | Explain the various hardware securities (Smartcard and Biometrics ). | A | 10 |
|  | Describe VPN and its types with a neat diagram. | U |  |
|  | Explain Security protocols SSL and TLS with a neat diagram. | U |  |
|  | Discuss IPSec with Authentication and ESP headers. | U |  |
| III | Explain infrastructure of IDS with a neat diagram. | U | 05 |
|  | Describe the classification of IDS. | U |  |
|  | Define IDS? List the functions performed by Intrusion Detection System. |  |  |
|  | Explain the need for firewalls. | U |  |
|  | Describe malicious software and its types. | U |  |
|  | List the types of firewalls. | R |  |
|  | Mention the limitations of firewalls. | R |  |
|  | Write a note on network based IDS. | U |  |
|  | Write a note on host based IDS. | U |  |

| | | | |
|---|---|---|---|
| | Write a note on Anomaly detection and signature detection. | **U** | **10** |
| | Describe misbehaviour signatures – signature detection with its disadvantages. | **U** | |
| | Explain Packet Filtering Firewall and its importance. | **A** | |
| | Explain host-dependent programs and host-independent programs. | **U** | |
| | Explain Proxy Firewall with a neat diagram. | **A** | |
| IV | Mention advantages of wireless network. | **R** | **5** |
| | Explain how to safeguard Wireless LANs. | **U** | |
| | Write a short note on Wireless LAN security. | **U** | |
| | List various WLAN configurations. | **R** | |
| | Explain WAP protocol architecture. | **U** | **10** |
| | Describe WAP security. | **U** | |
| **V** | Indicate the security of threats faced while using web. | **U** | **05** |
| | List the parameters of SSL session state. | **R** | |
| | List the parameters of SSL Connection state. | **R** | |
| | List the services provided by SSL record protocol. | **R** | |
| | Write a note on S-HTTP. | **U** | |
| | Write a note on Secure Electronic Transaction (SET). | **U,A** | |
| | Explain the client/server architecture of web. | **U** | **10** |
| | Describe web traffic security approaches. | **U** | |
| | Explain the importance of SSL/TLS for secure web services. | **U** | |
| | Explain the parameters of SSL session and SSL connection states. | **U** | |
| | Describe SSL record protocol with a neat diagram | **U** | |
| | Explain SSL handshake protocol | **U** | |
| | Explain the flow of transaction in SET with a diagram. | **U** | |
| | Describe the SET components and their relationships. | **U** | |
| **VI** | Write a short note on Indian Penal Code. | **U** | **05** |
| | Describe Information Technology act, 2000. | **U** | |
| | Explain the consumer protection act, 1986. | **U** | |
| | Discuss Consumer Protection Act. | **U** | |
| | Discuss the constituents of consumer complaint and its stakeholders | **U** | |
| | Describe network security aspects in E-Governance. | **U** | |
| | List the email threats that an organization face. | **R** | |
| | Explain the purpose of email policy. | **U** | |
| | Discuss initiatives undertaken by government to upgrade security standards. | **U** | **10** |
| | Describe Security monitoring tools. | **U** | |
| | Explain how an email system works with a diagram. | **U** | |
| | Explain how you create an email policy for your organization. | **U** | |