Govt. of Karnataka, Department of Technical Education
Diploma in Information Science & Engineering

Sixth Semester

Subject: Network Security & Management

Contact Hrs / week: 4 **Total hrs: 64**

Table of Contents

SN	Content	Hours	Marks
1	Introduction	2	5
2	Organizational Policy and Security	4	10
3	Security infrastructure	2	5
4	Cryptography	12	30
5	Hardware & Software Security	6	15
6	Intrusion Detection System	6	15
7	Network Security	12	30
8	Wireless Security	6	15
9	Security & law	2	5
10	Internet governance and electronics mail policy	4	10
	Seminars, Guest Lectures, Industry Visit and other Innovations	5	
	Tests	3	
	Total	**64**	**140+5 Objectives**

Detailed Contents

1		**Introduction**
1.1		Why Network Security is Needed
1.2		Management principles
1.3		Security principles
1.4		Network Management
1.5		Security Attacks
	1.5.1	Denial-of-Service (DoS)
	1.5.2	Information leakage
	1.5.3	Regular file access
	1.5.4	Misinformation
	1.5.5	Special File/Database access
	1.5.6	Remote arbitrary code execution
	1.5.7	Elevation of Principles
1.6		Qualities of Good Network
1.7		Internet Standards and the Internet Society (Ref page 267 of reference text)
2		**Organization Policy and Security**
2.1		Security Polices, Standards and Guidelines
2.2		Information Policy
2.3		Security Policy
2.4		Physical Security
2.5		Social Engineering
2.6		Security procedures
2.7		Building a Security Plan
	2.7.1	Elements of Security Plan
	2.7.2	Network Security Planning
3		**Security Infrastructure**
3.1		Infrastructure Components
	3.1.1	Network Category
	3.1.2	Platform category
	3.1.3	Physical Components
	3.1.4	Process Category
3.2		Goals of Security Infrastructure
	3.2.1	Data Confidentiality
	3.2.2	Data Integrity
	3.2.3	Data Availability
3.3		Design Guidelines
	3.3.1	Authentication
	3.3.2	Authorization
	3.3.3	Accounting
	3.3.4	Physical Access Controls
	3.3.5	Logical Access Controls

4		**Cryptography (Ref: Text 2)**
4.1		Symmetric Encryption Principles
4.2		Symmetric Block Encryption Algorithms
4.3		Random and Pseudorandom Numbers
4.4		Stream Ciphers and RC4
4.5		Cipher Block Modes of Operation
4.6		Approaches to Message Authentication
4.7		Secure Hash Function
4.8		Message Authentication Codes
4.9		Public Key Cryptography Principles
4.10		Public-Key Cryptography Algorithms
4.11		Digital Signatures
5		**Hardware and Software Security**
5.1		Hardware Security
5.2		Smart Cards
5.3		Biometrics
5.4		Virtual Private Networks
	5.4.1	Types of VPN’s
5.5		Trusted Operating Systems
5.6		Pretty Good Privacy (PGP)
5.7		Security Protocols
	5.7.1	Security Socket Layer
	5.7.2	Transport Layer Security
	5.7.3	IPSec
	5.7.4	S/MIME(Secure/Multipurpose Internet Mail Extension)
6		**Intrusion Detection System**
6.1		What is not an IDS?
6.2		Infrastructure of IDS
6.3		Classification of IDS
6.4		Host-based IDS
6.5		Network based IDS
6.6		Anomaly Vs Signature Detection
	6.6.1	Normal Behavior Patterns-Anomaly Detection
	6.6.2	Misbehavior Signatures-Signature Detection
	6.3.3	Parameter Pattern Matching
6.7		Manage an IDS
7		**Network Security**
7.1		Fundamental Concepts
	7.1.1	Objectives
		Assets
		Threats

		Vulnerability
		Safe Guards
		Attack
7.2		Identification and Authentication
	7.2.1	Proof by knowledge
		Proof by Possession
		Proof by Property
		Strong Authentication
7.3		Access Control.
	7.3.1	Identity - Based Policies
		Rule based Policy
		Security Requirements
		Mandatory Access Control
		Discretionary Access Control
		Labeling
		Auditing
		Convert Channel Analysis
7.4		A model of Network Security
	7.4.1	General Vulnerabilities
		Attacks on Internet Protocol
		Attacks on Internet Service
7.5		Malicious Software
	7.5.1	Safeguards
7.6		Firewalls
	7.6.1	Packet-Filtering Firewalls
		Stateful Inspection Firewalls
		Proxy firewalls
		Guard
		Personal Firewalls
		Limitations of Firewalls
8		**Wireless Security**
8.1		Wireless Application Protocol
8.2		WAP Security
	8.2.1	Authentication
	8.2.2	Integrity
		Confidentiality
8.3		Security Issues with Wireless Transport Layer Security (WTLS)
8.4		Wireless LAN
	8.4.1	WLAN Configuration
		WLAN Technology consideration
8.5		Wireless LAN Security
	8.5.1	Access Point Security
	8.5.2	Work Station Security
	8.5.3	Safeguarding Wireless LAN’s

9		**Security and Law**
9.1		Regulations in India
9.2		Information Technology Act, 2000
	9.2.1	Cyber Crime and the IT Act, 2000
9.3		Indian Contract Ac, 1872
9.4		Indian Penal Code
9.5		Indian Copyright Act
9.6		Consumer Protection Act, 1986
9.7		Specific Relief Act, 1963
9.8		Government Initiatives
9.9		Future Trends-Law of Convergence
10		Internet Governance and Electronic Mail Policy
10.1		Internet Governance
	10.1.1	The Infrastructure and Standardization
		Legal
		Economic
		Development
10.2		Network Security Aspects in E-Governance
	10.2.1	Why Securing E-Governance
		Security Measures and Threats
10.3		Security Monitoring Tools
	10.3.1	Vulnerability Assessment
		Security Policy Development
		Wireless Network Analysis
		Successful Identify Authentication
10.4		Electronic Mail
	10.4.1	Electronic Mailboxes and Addresses
		Mail Transfer
		How does E-mail work?
		Internet Mail Protocols
10.5		What are the E-mail Threats that Organization’s Face?
		Legal Liability
		Confidentiality Breaches
		Damage to Reputation
		Loss of Productivity
		Network Congestion and Down Time
		Email Retrieval on Court Order
10.6		Why do you Need an E-mail Policy?
10.7		How do you Create E-mail Polciy?
	10.7.1	E-mail Risks
		Best Practices
		Personal usage
		Wastage of Resources

		Prohibited Content
		Documentation Retention Policy
		Treatment of Confidential Data
		E-mail Monitoring
10.8		Publishing the E-mail Policy
10.9		University E-mail Policy
	10.9.1	Purpose and Scope
		Specific Provisions
		Campus Responsibilities and Discretion

Text Books:

1. **Network Security and Management**,2nd edition, Brijendra Sing, PHI, ISBN: 9788120339101 (Chap: 1,2,3,5,6,7,8,9,10)
2. **Network Security Essentials: Applications and Standards**, 3/e, William Stallings, Pearson, ISBN: 9788131716649 (Chap 4)

Reference:

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

General Objectives:

After the completion of the study of this subject students should be able to

1. Knows the concepts & basic vocabulary of network security, organization policy & security infrastructures .
2. Knows the various cryptographic algorithms & protocols along with hardware & software security
3. Knows how intursion detection systems works
4. Knows about WAP security & security issues with WTLS
5. Knows about the laws involved in security and polices

Specific Objectives:

1	**Introduction**
	Need for network security
	Learn the management and security principles
	Learn the various security attacks
	Learn the qualities of a good network
2	**Organization policy & security**
	learn the various policies and standard
	Design a security plan
3	**Security Infrastructures**
	Learn about the infrastructure components & category

	Learn the goals of security
	Design guidelines for providing security
4	**Cryptography**
	Learn the various terminologies used in cryptography
	Know the various encryption methods & how they work
	Learn various methods used in secret key cryptography, secret key cryptography, Hashing, public key cryptography and digital signatures
5	**Hardware and Software security**
	Learn how to provide a secure System
	Comprehend Hardware security features
	Learn the various Hardware security devices
	Learn the types of VPNs
	Learn the feature required for having a trusted OS
	Learn PGP
	Learn the various Protocols
6	**Intrusion and Detection System**
	Learn to differentiate between what is not an IDS and IDS
	Learn the infrastructure of IDS
	Learn the classification of IDS
	Learn about various IDS
	Disingvish between Anomaly and signature detection
	Learn the classification of detection
7	**Network Security**
	Learn the fundamental concepts of security
	Learn to identify and aunthenticate
	Learn the ways of Aunthenticated user identity
	Learn the policy involved in access control
	Learn security requirement
	Learn the model for network security
	Learn the general vulnerabilities
	Comprehend the attacks on internet protocol and internet services
	Know the catagories of malicious softwares
	Understand concepts of firwalls and their types
8	**Wireless security**
	Learn about WAP
	Learn the goals of WAP security
	Learn the security issues WTLS
	Learn wireless network architecture and various configuration
	Learn to use the technology concern to WLAN and its security
9	**Security and Law**
	Learn the regulation made by india
	Learn the IT act Contract act , Copy right act, protection act and relief act
	Comprehend the initiatives taken by GOVT
10	**Internet Governance and Electronic Mail policy**
	Learn the various network security acpects in E governance

	Learn security monitoring tools
	Understand how E mail works
	Learn the various internet Mail protocol
	Learn the E mail Threads and an organastion faces
	Comprehend the need for E mail policy
	Learn to create and publish Email policy

Govt. of Karnataka, Department of Technical Education

Diploma in Information Science & Engineering

Sixth Semester

Subject: Network Security and Management

Max. Marks: 100 Max. Time: 3 Hours

Model Question Paper

Note: 1. Section –I is compulsory.

1. Answer any TWO questions from each remaining Sections.

Marks

Section – I

1. a) Fill in the blanks with appropriate word/s 5x1=5

i.

ii.

iii

iv.

v.

b) Describe the Trusted OS 5

Section – II

2. a) Why network security is needed and How to maintain 5

b). Explain Information policy and their Classification 10

3. a) Explain the Goals of security infrastructure 5

b) With a neat diagram explain Feistel Cipher Structure and its design elements 10

4. a) What are the requirements of Hash function 5

b) Explain RSA algorithm with example 10

Section – III

5. a) Write a short note MD5 message digest 5

b) Explain the various hardware securities 10

6. a) Explain pretty good privacy 5

b) Describe the classification of IDS 10

7. a) Write a note on Signature detection 5

b) Explain pocket filtering Firewall 10

Section – IV

8. a) Explain limitation of Firewall 5

b) Explain the model for Network security 10

9. a) What is access point? Explain access point security 5

b) Explain several ways to configure WLAN 10

10. a) Explain indian copy right act 5

b) Explain how to publish an E mail policy for an organization 10