# GUJARAT TECHNOLOGICAL UNIVERSITY
## MASTER OF COMPUTER APPLICATIONS (MCA)
## SEMESTER: V

Subject Name: **Network Security (NS)**
Subject Code: **650002**

---

### Learning Objectives:

After completion of this course student will be able to appreciate

- What security threats and attacks are and what are the counter measures
- Symmetric and asymmetric encryption methods
- Authentication applications, Web, IP and Email security
- Intruders and Firewalls

### Prerequisites:

- Fundamentals of Networking
- Number theory
- Basic Mathematics

### Contents:

1. **Network Security and Symmetric Encryption** **[20%]**
   Security Trends, The OSI Security Architecture, Security Attacks, Security Services, Security Mechanism, A Model for Internetwork Security, Internet Standards the Internet Society. Symmetric Encryption Principles, Symmetric Block Encryption Algorithms, Stream Ciphers and RC4, Cipher Block Modes of Operation, Location of Encryption Devices, Key Distribution.

2. **Public Key Cryptography and Authentication** **[20%]**
   Approaches to Message Authentication, Secure Hash Functions and HMAC, Public Key Cryptography Principles, Public Key Cryptography Algorithms, Digital Signatures, Key Management. Kerberos, X.509 Directory Authentication Service, Public Key Infrastructure.

3. **Email and IP Security** **[20%]**
   Pretty Good Privacy (PGP), S/MIME.
   Overview of IP Security, IP Security Architecture, Authentication Header, Encapsulating Security Payload, Combining Security Associations, Key Management.

4. **Web Security and Intrusion** **[20%]**
   Web Security Requirements, Secure Sockets Layer (SSL) and Transport Layer Security (TLS), Secure Electronic Transaction (SET). Intruders, Intrusion Detection.

5. **Passwords and Firewalls** **[20%]**
   Password Management. Firewall Design Principles, Trusted Systems, Common Criteria for Information Technology Security Evaluation.

## Text Book (Theory):

1) William Stallings, "Network Security Essentials: Applications and Standards", 3rd Edition, Pearson Education.

## Other Reference Books (Theory):

1) Behrouz Forouzan, "Cryptography and Network Security", TMH Publication.
2) Nina Godbole, "Information Systems Security", Wiley Publication.
3) William Stallings, "Cryptography and Network Security", Pearson Education.

## Chapter wise coverage from the Text Book:

| Chapter No. | Topics/Subtopics | No. of Lectures |
|---|---|---|
| 1 | * | 02 |
| 2 | * | 05 |
| 3 | * | 07 |
| 4 | * | 07 |
| 5 | * | 06 |
| 6 | * | 06 |
| 7 | * | 06 |
| 9 | * | 05 |
| 11 | * | 04 |
| | **Total No. of Lectures** | 48 |

* All topics/subtopics from the given chapter to be included in syllabus

## Accomplishments of the student after completing the Course:

- Understand and appreciate the importance of Network Security in today's world.
- Understand and use good Network Security applications and standards in various applications.

---

**PROPOSED CEC ACTIVITIES**

**Exploratory Activities:**

1. Identify different network security attacks that can be launched on a network. Describe the modus operandi of these attacks. Clearly mention the layer/s at which these attacks operate. Identify the security vulnerabilities in the network protocol stack because of which the attack became possible. Finally, mention the solutions currently in use to thwart these attacks.
2. Survey the security features (both network and system security) available in popular web browsers like IE, Google Chrome, Mozilla FireFox and Opera. Prepare a comparative report on your findings.
3. Survey the security features (both network and system security) available in popular desktop operating systems Windows XP, Windows 7 and RedHat Linux. Prepare a comparative report on your findings.
4. Survey the security features (both network and system security) available in popular server operating systems Windows 2003 Server and RedHat Linux (Enterprise) Server. Prepare a comparative report on your findings.

5. Study in detail the personal firewall provided in Windows XP and prepare a technical report on it. Also, survey the built in packet filtering facility available in Linux – IPTABLES and prepare a report on it.
6. Survey the security features available in popular web based email service providers like gmail, yahoo, hotmail etc. Prepare a technical report on it.
7. Study in detail the enterprise firewall (eg. Cyberoam from Elitecore Technologies) of your college and prepare a report on it.
8. Install GNU Privacy Guard, configure it and show how PGP encrypted email can be sent and received. Show how GNU Privacy Guard can be used to encrypt and decrypt files on hard disk. Install a PGP plug-in for MS Outlook Express, appropriately configure MS Outlook Express and hence, show how PGP encrypted emails can be sent and received.
9. Survey network security features used in application layer software like CuteFTP, FileZilla FTP, MS-OutlookExpress and SSH and prepare a technical report on them.
10. Prepare a technical report on network security features available in wireless devices like GSM (with /without wifi) mobile phones as well as stand-alone wi-fi devices like AP, router, etc.
11. Survey popular Anti-Virus solutions like Kaspersky, Avast, AVG, e-trust, McAfee, Trend Micro PC-Cillin, Norton, etc. and prepare a comparative report about their features.
12. Prepare a report on the different types of log files that get generated by: a) Client OS b) Server OS in your network. Understand the purpose of each column in that particular file (log file format). Refer to the technical documentation of the OS for its explanation. Now, carry out different network related activities like purposely making 3 failed logins, taking a print out, copying a file, etc. and examine the entries in the log files corresponding to these activities.
13. Prepare a report on the SNORT Intrusion Detection System.
14. Security testing is an important aspect of Software Testing. Find out different kinds of security tests which the software of a typical web based system normally needs to undergo.
15. Survey popular programming languages like C, C++ and Java and identify bad code development practices which might result into security flaws.
16. Prepare a technical report on the working of any one popular Internet based online payment systems like PayPal and the security features in it.
17. Write a technical report on " Credit Card System Security"

## Programming Oriented Activities:

Here, some real life Network Security related scenarios/problems are given. Students are supposed to follow the given instruction for solving them.

**General Instructions: -**

a) There are probably more than one ways to solve following problems. You are supposed to find out the best possible solution to the problems. You may be required to prove that the solution provided by you is better than other alternatives.
b) These scenarios are intended to help the students to visualize which security objectives and mechanisms would be required under different real life IT security scenarios.
c) All the programs should be implemented based upon Java Socket Programming and Java cryptography/security related packages.
d) The algorithms to be used are shown as under

**Confidentiality:**
DES, 3DES, AES (with ECB,CBC, CFM, Stream Cipher mode), RC4, RSA

**Message Authentication/Message Integrity**
MD5, SHA, HMAC

**Key Exchange**
Diffie Hellman/RSA

**Session encryption**
SSL (simple programs like echo, chat, daytime based on SSL requiring confidentiality only)

**Digital Signatures**
RSA with SHA/MD5

## SCENARIOS

1. Suppose an anonymous Intranet based student's feedback system is to be implemented in Java. It is required that nobody should be able to interpret the contents of the feedback except the principal. What security services would be required in this system? What security mechanism/s could be used to achieve the above security objectives? Based upon your answers, implement the same using Java using socket programming and appropriate security related java packages. The principal should not be able to find out who has given a specific feedback.

**Hint:**
In above program, since the feedback is meant to be anonymous so authentication or non repudiation is not required. Confidentiality is the most important issue in this scenario. Eg. DES can be used.

1. Suppose a college canteen wants to create an Intranet based ordering system in which staff and students can book their orders. Which security services would be desirable in such system? Which are the mechanisms which would help to achieve these security objectives? Based upon your answers, implement the same in Java using socket programming and security related java packages.

**Hint:**
In above program, confidentiality is obviously not required. Moreover, the risk involved in such transaction is not so high that digital signature is required. However, authentication would be necessary. Eg. HMAC-md5 could be used.

2. Suppose an Internet based real time interaction program like "Talk with CM" is to be developed where any anonymous citizen can complain regarding corporations, Govt. officials, MLAs, etc. Which security services would be desirable in such system which should protect such whistleblowers so much so that nobody should ever be able to find out their identity? Which are the mechanisms which would help to achieve these security objectives? Based upon your answers, implement the same in Java using socket programming and security related java packages.

**Hint:**
In above program, since the identity of the citizen need not be revealed, hence, authentication is not required. However, confidentiality is required so as to enable the CM to catch the culprits/negligent govt. staff unawares. Moreover, the encryption algorithm used should be suitable for interactive/real time kind of communication. (eg. Stream cipher like RC4)

3. Suppose there are around 100 people in a group who want to communicate mutually in a secure way. However, one major issue would be: How many no. of keys would be required? Suggest some innovative way so that everybody can mutually communicate with each other confidentially and yet the no. of keys required is manageable. Based upon your answers, implement the same in Java using socket programming and security related java packages.

**Hint:**
In such situations, it is better to take help of public key based methods. Eg. RSA. Thus, everybody in the group would have a pair of keys: public and private. When any two persons want to communicate confidentially, they may exchange the secret shared session key using RSA. This will save the labor of maintaining very large no. of symmetric keys. [n . (n-1)!/2 in this case] As value of n increases, the problem of managing the symmetric keys becomes more and more severe.

4. Suppose A and B want to communicate with each other confidentially. Both A and B would be sending and receiving large files as data. One issue for A is to communicate the secret key to B which helps decrypt the file. *In no case should the key be transmitted in plaintext*. Moreover, it is expected that business data communications between A and B should not only be confidential but also be reasonably speedy. Which security services would be desirable in such system? Which are the mechanisms which would help to achieve these security objectives? Based upon your answers, implement the same in Java using socket programming and security related java packages.

**Hint:**
In above program, one may use RSA or Diffie-hellman to exchange the symmetric key securely and then use come block cipher like DES, 3DES or AES

5. Suppose a secure channel is to be established between Ministry of Defense and the Army headquarters. This communication channel is supposed to be used not only under normal situations but also during war, rescue operations, etc. Which security services would be desirable in such system? Which are the mechanisms which would help to achieve these security objectives? Based upon your answers, implement the same in Java using socket programming and security related java packages. Though you may not be able to implement currently, can you suggest what type of other issues need to be managed in this case? Elaborate few of them and try answering them.

**Hint:**
In above program, since the communication is extremely sensitive and affects the security of the entire nation, so all the major security services like message confidentiality, message authentication, message integrity and non repudiation would be required. We neglect the issue of entity authentication in this scenario just to keep the program simple, even though, it would also be definitely required if such system would be deployed for actual use. Instead of providing the above services separately, one may opt to use SSL for providing various security services to the entire session.

6. Suppose a company is required to deliver educational services like e-education on payable basis through the Internet. Company may provide online as well as offline training (eg. Live lecture/demo session as well as delivering recorded sessions to be used on offline basis). Which security services would be desirable in such system? Which are the mechanisms which would

help to achieve these security objectives? Based upon your answers, implement the same in Java using socket programming and security related java packages.

**Hint:**
In above program, since the services are paid, so the delivery of educational material whether offline or online should be done confidentially. Hence, block cipher like DES, 3DES or AES may be used. However, for online delivery, RC4 is preferable because of better delay characteristics. Also, authentication is required on the company's side before delivering the services since the services are paid. Hence, HMAC-SHA1 might be used.

7. Bob signs his will and sends it to his lawyer Alice. Which security services would be desirable in such system? Which are the mechanisms which would help to achieve these security objectives? Based upon your answers, implement the same in Java using socket programming and security related java packages.

**Hint:**
In above program, confidentiality might not be necessary. However, authentication and non repudiation is necessary. Hence, digital signature is required.

8. Suzan is a raw material supplier for Sam. Sam places an order of 1000 units to Suzan through Internet. Which security services would be desirable in such system? Which are the mechanisms which would help to achieve these security objectives? Based upon your answers, implement the same in Java using socket programming and security related java packages.

**Hint:**
In above program, neither Sam nor Suzan should be able to repudiate their involvement in this transaction. Hence, digital signature would be required.

9. Neil wants to send confidential information to Scott from time to time. However, whenever this communication needs to be done, a fresh new symmetric key has to be communicated to Scott. *The symmetric key should not be transmitted in plaintext in any case.* Which security services would be desirable in such system? Which are the mechanisms which would help to achieve these security objectives? Based upon your answers, implement the same in Java using socket programming and security related java packages.

**Hint:**
In above program, one may use RSA or Diffie-Hellman to exchange the symmetric key securely and then use come block cipher like DES, 3DES or AES in CBC mode.

10. Sam wants to send a message to Peter in a network. Peter on receiving the message wants to confirm that the message is actually coming from Sam only as well as the contents of the message has not been altered. Which security services would be desirable in such system? Which are the mechanisms which would help to achieve these security objectives? Based upon your answers, implement the same in Java using socket programming and security related java packages.

**Hint:**
In above program, message authentication as well as message integrity is required. Hence, one may use HMAC-md5.