Noorul Islam College of Engineering
Department of Electronics and Communication Engineering

M.E Communication Systems
CO1630-Communication Network Security

Prepared by G.Arockia Selva Saroja
AP/ECE

Unit-1: Symmetric Ciphers

2 mark questions

1. Define security attack ?

Any pattern that compromise the security of information owned by an organization is called as the security attack.

2. Define security mechanism ?

A mechanism that is designed to detect, prevent or recover from security attacks.

3. What do you mean by security service ?

A service that enhances the security of data processing systems and information transfer of an organization.

4. What are the classifications of security services ?

(a). Confidentiality
(b). Authentication
(c). Integrity
(d). Non-repudiation
(e). Access control
(f). Availability

5. What do you mean by confidentiality ?

This ensures that information in a computer system and transmitted information are accessible only for reading by authorized parties.

6. Define authentication ?

This ensures that origin of a message or electronic document is correctly identified with an assurance that identity is not false.

7. Define integrity ?

This ensures that every authorized parties are able to modify computer system assets and transmitted information.

8. What do you mean by non-repudiation ?

This means that neither the sender or the receiver message be able to deny the transmission.

9. What do you mean by access control ?

Access control requires that access to information resources may be controlled by the target system.

10. What are the types of security attacks ?

(a). Interruption
(b). Interception
(c). Modification
(d). Fabrication

11. What do you mean by interruption ?

An asset of system is destroyed or becomes unusable. This is an attack on availability.

12. What do you mean by interception ?

An unauthorized party gains access to an asset. This is an attack on confidentiality.

13. What do you mean by modification ?

An unauthorized party not only gains access to but tampers with an asset. This is an attack on integrity.

14. What are the types of attacks ?

(a). Active attacks
(b). Passive attacks

15. Define cryptography ?

Many schemes used for encryption constitute the access of study known as cryptography.

16. What do you mean by cryptanalysis ?

The process of attempting to discover plaintext or encryption key or both plaintext and encryption key is known as cryptanalysis.

17. What do you mean by steganography ?

Steganography is the process of concealing the existence of message. It is an encryption process.

18. What are the steganographic methods ?

(a). Character marking
(b). Invisible ink
(c). Pin punctures

(d). Type writer ribbon correction.

19. Name the techniques involved in classical encryption ?
(a). Substitution techniques
(b). Transposition techniques
(c). Rotor machines

20. What do you mean by stream cipher ?
A stream cipher is that one encrypts data stream one bit or one byte at a time.
eg: vernam cipher

21. What do you mean by block cipher ?
Here a block of plaintext is treated as a whole to produce a ciphertext block of equal length.

22. What do you mean by conventional encryption ?
Conventional encryption also referred to as symmetric encryption or single key encryption. The security of conventional encryption depends on several factors, such as the encryption algorithm and the secrecy of the key.

23. When do we say an encryption scheme is unconditionally secure ?
An encryption scheme is unconditionally secure if the ciphertext generated by the scheme does not contain enough information to determine uniquely the corresponding plaintext, no matter how much ciphertext is available.

24. When do we say an encryption scheme is computationally secure ?
An encryption scheme is computationally secure if they meet two criterias.

(a). The cost of breaking the cipher exceeds the value of the encrypted information.
(b). The time required to break the cipher exceeds the useful time of the information.

25. What is the strength of DES ?
The strength of DES depends on two factors.
(a). The use of 56-bit keys
(b). the nature of the DES algorithm.

Essay questions

1. Write about various security attacks, services and security mechanisms ?
2. What do you mean by symmetric cipher model ?

3. Describe about DES and it's strength ?
4. What are the block cipher design principles ?
5. Write about the various substitution techniques ?

Unit-2: Symmetric Ciphers

2 mark questions

1. What do you mean by avalanche effect ?

A desirable property of many encryption algorithm is that a small change in either a plaintext or key should produce a significant change in ciphertext.ie, a 1 bit change of plaintext or 1 bit change of key should produce a large change in ciphertext.

2. Expand IDEA ?

International Data Encryption Algorithm

3. Expand DES ?

Data Encryption Standard

4. What are the advantages of DES ?

(a). Improved efficiency
(b). Secure algorithm for DES is Rijndael.

5. What are the evaluation criteria for AES ?

(a). Security
(b). Cost and algorithm
(c). Implementation characteristics

6. What are the characteristics of Rijndael algorithm ?

(a). Resistance to all attacks
(b). Design simplicity
(c). Speed and code compactance

7. What is master key ?

The session key transmitted in encrypted form using master key that is shared by the key distribution center and an end system or user.

8. What is session key ?

Communication between end systems is encrypted using a temporary key called session key. This is used only during duration of logical connection and then it is discarded. Session key obtained from the key distribution center.

9. How keys are classified based on usage ?

(a). PIN(Personal Identification Number): encryption key used for electronic and transfer.
(b). File encrypting for encrypting publicly accessible locations.

10. What do you mean by confusion in IDEA ?

Ciphertext depends on plaintext and key in a complicated way. The objective is to complicate the determination how the statics of the ciphertext depend on the statics of p[laintext.

11. How confusion is achieved ?

Confusion is achieved by mixing three different operations(two 16 bit) to produce a single output.

The operations are,

(a). Bit by bit exclusive OR
(b). Addition of integers modulo
(c). Multiplication of integers modulo 2^16+1.

12. What is diffusion in IDEA ?

The plaintext should influence the ciphertext and key should influence ciphertext. This is called diffusion.

13. List the characteristics of Blowfish ?

(a). Fast
(b). Compact
(c). Simple
(d). Variably secure

14. List the characteristics of RC5 ?

(a). Fast
(b). Variable number of rounds
(c). Simple
(d). Less memory requirement
(e). High security

15. What are the characteristics of advanced block ciphers ?

Variable key length, nixed operators, data dependent rotation, variable number of rounds, key dependent S boxes.

16. Differentiate link encryption and end to end encryption ?

Link encryption	End to end encryption
(a). Message exposed in Sending host.	(a). Message encrypted in Sending host.
(b). One facility for all users.	(b). User must determine the algorithm.
(c). Transparent to user.	(c). User applies encryption.
(d). Requires one key per	(d). Requires one key per

host intermediate node. user pair.

17. What are the parameters of RC5 ?
w: word size in bits. RC5 encrypts 2 word blocks
r: number of rounds
b: number of 8-bit bytes(octets) in secret key k.

18. List the information obtained from traffic analysis attack ?
(a). Identities of parties
(b). Message pattern, message length
(c). How frequently parties communicate

19. What do you mean by key distribution ?
For encryption, the same keys are shared by the sender and the receiver. For this, a set of keys is being used called key distribution.

20. What are the uses of random numbers ?
(a). Reciprocal authentication scheme
(b). Session key generation.
(c). Generation of keys for RSA public key encryption algorithm.

21. Expand BBS & CSPRBG ?
BBS-Blum Blum Stub generator.
CSPRBG-Cryptographically Secure Pseudo Random Bit Generator.

22. What are the operations used in RC5 ?
RC5 uses three primitive operations. They are,
(a). Addition
(b). Bitwise exclusive OR
(c). Left circular rotation

23. What is a transparent key control scheme ?
A transparent key control scheme is useful for providing end to end encryption at a network or transparent level in a way that is transparent to the end users.

24. Mention the four stages used in AES ?
AES uses four stages. One permutation and three substitution stages.
(a). Substitute bytes
(b). Shift rows
(c). Mix columns
(d). Add round key

25. What is meet in the middle attack ?

The algorithm known as meet in the middle attack is based on the observation that is we have, C = Ek2[Ek1(P)]

Then,

X = Ek1[P] = Dk2[C]

Essay questions

1. What are the evaluation criteria for AES ?
2. Write about AES cipher ?
3. Describe briefly about the block cipher modes of operation ?
4. What do you mean by stream ciphers and explain RC4 & RC5 algorithms?
5. Write about IDEA and Blowfish ?

Unit-3: Public key encryption and Hash functions

2 mark questions

1. What are the characteristics of public key algorithms ?
   (a). Computationally infeasible
   (b). Either of two related keys can be used for encryption with others used for decryption.

2. Requirements of key distribution ?
   (a). Share a key, which is being distributed
   (b). Use of key distribution center

3. Differentiate conventional & public key encryption ?

Conventional encryption	Public key encryption
(a). Same key used for encryption and decryption	(a). Pair of keys is used
(b). Key must be secure	(b). One of the two keys is kept secure
(c). Sender and receiver must Share the algorithm and key.	(c). Should have one matched Pair of keys.

4. What do you mean by one way function ?

One way function maps a domain into a range such that every function value has a unique inverse with condition,

Y=f(X), easy to calculate.

X= f^-1(Y), infeasible.

5. Define trap door one way function ?

Trap door one way function is easy to calculate in one direction and infeasible to calculate in another direction unless certain additional information is known.

6. What are the types of attacks on RSA ?
   (a). Brute force attack
   (b). Mathematical attacks
   (c). Timing attacks

7. Name the method by which timing attacks can be avoided ?
   (a). Constant exponentiation time
   (b). Random delay
   (c). Blinding

8. What is the need for Diffie-Hellman key exchange ?

This enables users to exchange a key securely that can be used for subsequent encryption of messages.

9. What are the techniques for distribution of public keys ?
   (a). Public announcement
   (b). Public available directory
   (c). Public key authority
   (d). Public key certificates

10. What do you mean by ECC ?

ECC(Elliptic Curve Cryptography) appears to offer equal security for smaller bit size thereby reducing processing overhead.

11. Expand RIPEMD-160 ?

RACE Integrity Primitives Evaluation(RIPE) project.

12. What are HMAC design objectives ?
   (a). To use without modifications available hash functions
   (b). To preserve original performance of hash function
   (c). To use and handle keys in a simple way

13. What are the properties of digital signatures ?
   (a). Ensures time, date and author of the actual message
   (b). Able to authenticate the contents of message at the time of signature
   (c). Digital signature is an authentication protocol

14. What are the requirements of digital signature ?
   (a). Computationally infeasible
   (b). Easy recognition
   (c). Practical to regain the copy of digital signature

15. Define MAC ?

An alternative authentication technique involves the use of a secret key to generate a small fixed size block of data, known as cryptographic checksum or MAC. This technique assumes two communicating parties say A and B share a common secret key k.

16. Define Hash function ?

A variable on the message authentication code is the one-way hash function. As with the message authentication code, a hash function accepts a variable size message M as input and produces a fixed size hash code H(M), sometimes known as a message digest as output.

17. What are the processing steps in MD5 logic ?

(a). Append padding bits
(b). Append length
(c). Initialize MD buffer
(d). Process the message in 512 bit blocks
(e). Output

18. What are the goals of MD4 ?

(a). Security
(b). Speed
(c). Simplicity and compactness
(d). Favor little endian architecture

19. What is a replay attack ?

Replay attacks allow an opponent to compromise a session key or successfully impersonate another party, and is said to be a replay attack.

20. Name the two aspects to the use of public key encryption ?

(a). The distribution of public keys
(b). The use of public key encryption to distribute secret keys.

21. Advantages of cryptography with elliptic curve ?

When compared with RSA algorithm, ECC have,

(a). Smaller key length
(b). Simple computation
(c). Easy implementation in software and hardware

22. What is meant by message authentication ?

Message authentication is a procedure to verify the received messages come from the alleged source and have not been altered. Message authentication may also verify sequencing and timeliness.

23. What are the authentication requirements ?

The authentication requirements in the context of communications across a network, the following attacks can be identified.

(a). Disclosure
(b). Traffic-analysis
(c). Masquerade
(d). Content modification
(e). Sequence modification
(f). Timing modification
(g). Repudiation

24. Define a weak collision resistance and a strong collision resistance ?

Weak collision resistance

For any given block x, it is computationally infeasible to find $y \neq x$ with the hash value function $H(y) = H(x)$. This is sometimes referred to as weak collision resistance.

Strong collision resistance

It is computationally infeasible to find any pair (x, y) such that $H(x) = H(y)$. This is referred to as strong collision resistance.

25. What is meant by a birthday attack ?

The strong collision property of a hash function refers to how resistant the hash function is to a class of attack known as the birthday attack.

Essay questions

1. What do you mean by Public key cryptography and explain the RSA algorithm and it's security mechanisms ?
2. What do you mean by key management ?
3. Write about the Diffie-Hellman key exchange algorithm ?
4. What is meant by ECC ?
5. Compare MD5 & SHA algorithms ?
6. What do you mean by Digital Signatures ? Describe about the digital signature standards(DSS) ?

UNIT: IV NETWORK SECURITY PRACTICE

Part A

1. Define Kerberos?

Kerberos is an authentication service designed for use in a distributed environment. Kerberos make use of a trusted third-part authentication service that enables clients and servers to establish authenticated communication.

2. What are the requirements of Kerberos?

Kerberos should have the following requirements

(a) Secure
(b) Reliable
(c) Transparent
(d) Scalable

3. What do you mean by Kerberos realm?

A full-service Kerberos environment consisting of a Kerberos server, a number of clients, and a number of application servers which satisfies the condition

(a) All users should be registered with the Kerberos server.

(b) All servers are registered with the Kerberos server.

Such an environment is referred to as a Kerberos realm.

4. Difference between Kerberos v4 and v5? (Environmental short comings of v4)

Version 4	Version 5
1. Encryption system dependence: Require the use of DES. 2. Internet protocol dependence: Use IP address other address types are not supported. 3. Ticket lifetime: Maximum life time 21 hours. 4. Authentication forwarding V4 does not support this 5. Message byte ordering: V4 chooses its own byte ordering scheme. 6. Interrealm authentication: Supports N^2 Kerberos to Kerberos relationships.	1. Encryption system dependence: Any encryption text may be used. 2. Internet protocol dependence: Allow any network type to be used. 3. Ticket lifetime: Uses an explicit start and end time i.e., tickets with arbitrary life times. 4. Authentication forwarding: V5 provides this capability. 5. Message byte ordering: V5 uses ASN.1 and BER 6. Interrealm authentication: Supports only fewer relationships.

5. Define X.509?

X.509 defines a format for public key certificates. It defines a framework for the provision of authentication services by the X.500 directory to its users.X.509 is based on the use of public-key cryptography and digital signatures.

6. Define PGP?

PGP is an open-source freely available software package for e-mail security. It provides authentication through the use of digital signature, confidentiality through the use of symmetric block encryption, compression using ZIP algorithm, e-mail compatibility using the radix-64 encoding scheme, and segmentation and reassembly to accommodate long e-mails.

7. What are the reasons for the popularity of PGP?

(a) It is available free worldwide in versions that run on a variety of platforms.
(b) It is based on algorithms that have survived extensive public review and are considered extremely secure.
(c) It has a wide range of applicability.
(d) It is not developed or controlled by any organization. For those with an instinctive distrust of the establishment this makes PGP attractive.
(e) PGP is now on an internet standards track.

8. What are the services offered by PGP?

PGP offers five services. They are:

(a) Authentication
(b) Confidentiality
© Compression
(d) E-mail compatibility and
(e) Segmentation

9. Define S/MIME?

S/MIME (Secure/Multipurpose Internet Mail Extension) is a security enhancement to the MIME Internet e-mail format standard, based on technology from RSA Data security.

10. What are the limitations of the SMTP/822 scheme?

1. SMTP cannot transmit executable files or other binary objects.

2. SMTP cannot transmit text data that contains national language characters.

3. SMTP servers may reject mail message over a certain size.

4. SMTP gateways that translate results in certain translational problems.

5. SMTP gateways to X.400 electronic mail networks cannot handle non-textual data included in X.400 messages.

6. Some SMTP implementations do not adhere completely to the SMTP defined in RFC 821.

11. What are the MIME specifications?

MIME specification includes the following:

1. Five new header fields are defined, which may be included in RFC 822 header.

2. A number of content formats are defined, thus standardizing representations that support multimedia electronic mail.

3. Transfer encodings are defined that enable the conversion of any content format into a form that is protected from alteration by the mail system.

12. What are the functions of S/MIME?

S/MIME provides the following functions:

- Enveloped data
- Signed data
- Clear-signed data
- Signed and enveloped data

13. What are the steps for preparing an enveloped data for a MIME entity?
    1. Generate a pseudorandom session key for a particular symmetric encryption algorithm.
    2. For each recipient, encrypt the session key with the recipient's public RSA key.
    3. For each recipient, prepare a block known as Recipient info.
    4. Encrypt the message content with the session key.

14. What are the steps for preparing a signed data MIME entity?
    1. Select a message digest algorithm.(SHA or MD5)
    2. Compute the message digest, or hash function, of the content to be signed.
    3. Encrypt he message digest with the signer's private key.
    4. Prepare a block known as signer info.

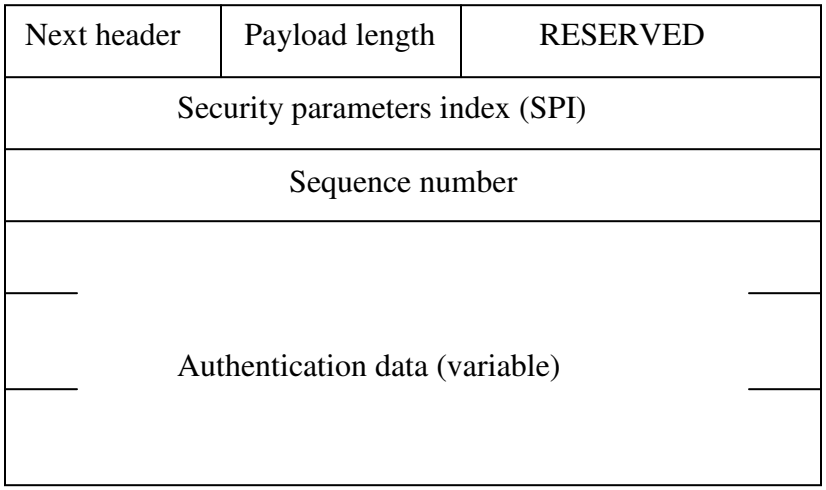
15. What are the applications of IPSec?

IPSec provides:

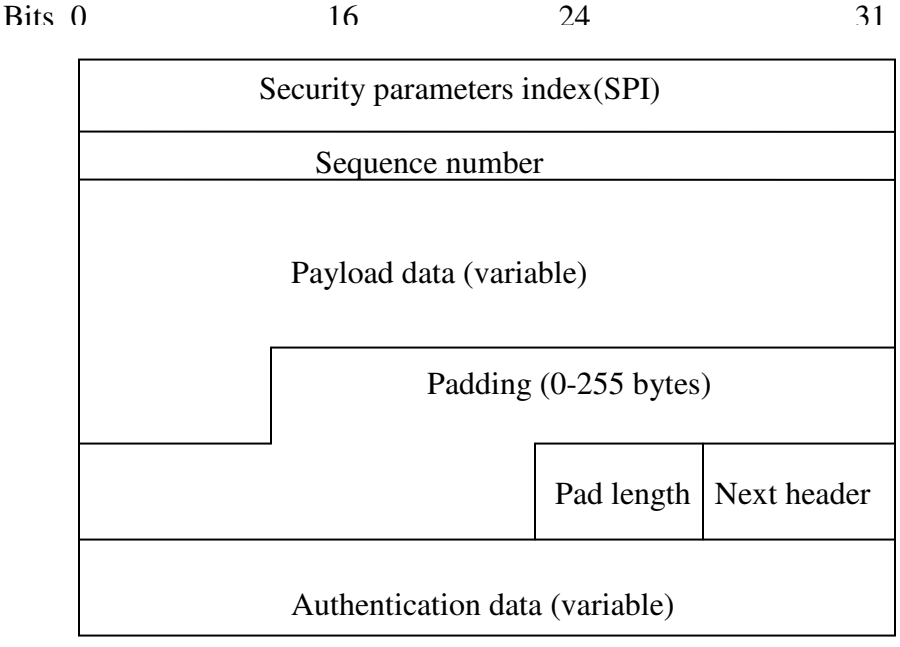
1. Secure branch office connectivity over the internet.
2. Secure remote access over the internet.
3. Establishing extranet and internet connectivity with partners.
4. Enhancing electronic commerce security.

16. What are the benefits of IPSec?
    1. When IPSec is implemented in a firewall or router, it provides a strong security.
    2. IPSec in a firewall is resistant to bypass if all traffic from outside must use IP.
    3. IPSec is below transport layer and is o transparent o users.
    4. IPSec can be transparent to the end users.
    5. IPSec can provide security for individual users if needed.

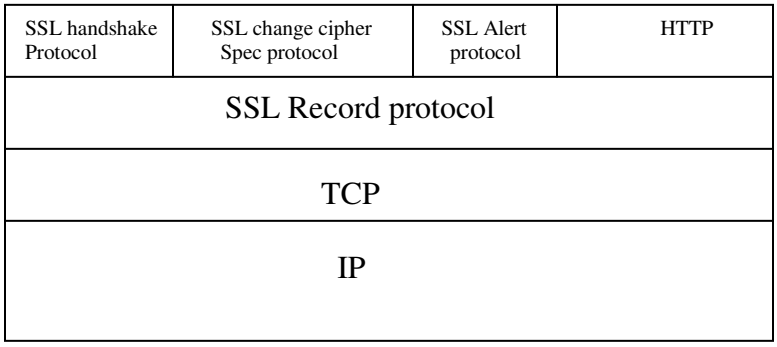
17. Draw the IPSec authentication header?



18. Draw the IPSec ESP format?



19. Draw the SSL protocol stack?



20. Define SSL?

Secure socket layer (SSL) provides security services between TCP and applications that use TCP. The internet standard version is called transport layer service (TLS).

21. Define SET?

Secure Electronic Transaction (SET) is an open encryption and security specification designed to protect credit card transactions on the internet. It is a set of security protocols and formats that enables users to employ the existing credit card payment infrastructure on an open network.

22. What are the services offered by SET?

SET provides 3 services:

1. Provides a secure communications channel among all parties involved in a transaction.
2. Provides trust by the use of X.509v3 digital certificates.
3. Ensures privacy because the information is only available tp parties in a transaction when and where necessary.

23. What are the requirements of SET?

1. Provide confidentiality of payment and ordering information.
2. Ensure the integrity of all transmitted data.
3. Provide authentication that a cardholder is a legitimate user of a credit card account.
4. Provide authentication that a merchant can accept credit card transactions through its relationship with a financial institution.
5. Ensure the use of best security practices and system design techniques to protect all legitimate parties in an electronic commerce transaction.
6. Create a protocol that neither depends on transport security mechanisms nor prevents their use.

7. Facilitate and encourage interoperability among software and network providers.

24. What are the key features of SET?

1. Confidentiality of information.
2. Integrity of data.
3. Cardholder account authentication.
4. Merchant authentication.

25. Name the SET participants?

1. Cardholder
2. Merchant
3. Issuer
4. Acquirer
5. Payment gateway
6. Certification Authority (CA)

26. What is the need for dual signature in SET?

SET uses dual signature. The purpose of the dual signature is to link two messages that are intended for two different recipients.

Part B

1. Explain the authentication service provided by Kerberos?
2. Explain X.509 authentication service?
3. Briefly explain PGP?
4. Explain S/MIME?
5. Explain the IPSec architecture?
6. Explain SSL and TLS?
7. Explain the payment processing of SET?

UNIT V SYSTEM SECURITY

Part A

1. What are the types of intruders?
   Three types of intruders are:
   (a) Masquerader
   (b) Misfeasor and
   (c) Clandestine user
2. Define masquerader?
   An individual who is not authorized to use the computer and who penetrates a system's access controls to exploit a legitimate user's account.
3. Define misfeasor?
   A legitimate user who access data, programs, or resources for such access is not authorized, or who is authorized for such access but misuses his or her privileges.
4. Define clandestine user?

An individual who seizes supervisory control of the system and uses this control to evade auditing and access controls or to suppress audit collection.

5. What are the techniques used for learning passwords?
    1. Try default passwords used with standard accounts that are shipped with the system.
    2. Exhaustively try all short passwords.
    3. Try words in the system's online dictionary or a list of likely passwords.
    4. Collect information about users.
    5. Use a Trojan horse.
    6. Tap the line between a remote user and the host system.

6. What are the approaches used for intrusion detection?

1. Statistical anomaly detection: Involves the collection of data relating to the behavior of legitimate users over a period of time.
2. Rule-based detection: Involves an attempt to define a set of rules that can be used to decide that a given behavior is that of an intruder.

7. What are the approaches used for statistical anomaly detection?

(A) Threshold detection: This approach involves defining thresholds, independent of user, for the frequency of occurrence of various events.
(B) Profile based: A profile of the activity of each user is developed and used to detect changes in the behavior of individual accounts.

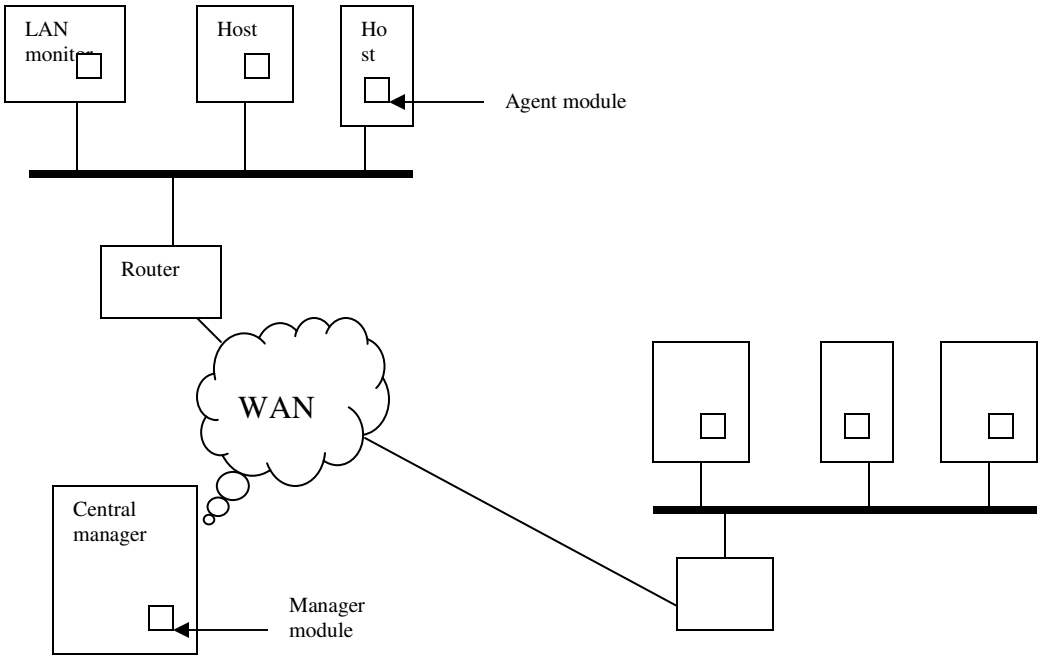
8. What are the approaches used for rule-based detection?

(A) Anomaly detection: Rules are developed to detect deviation from previous usage patterns.
(B) Penetration identification: An expert system approach that searches for suspicious behavior.

9. What are the various statistical tests used?

1. Mean and standard deviation
2. multivariate
3. Markov process
4. Time series
5. Operational

10. Draw the architecture for distributed intrusion detection?



11. How the ID provides security?

1. The ID determines whether the user is authorized to gain access to a system.
2. The ID determines the privileges accorded to the user.
3. The ID is used in what is referred to as discretionary access control.

12. What are the password selection strategies?

Four basic techniques used for password selection are:

1. User education
2. Computer-generated passwords
3. Reactive password checking
4. Proactive password checking

13. What do you mean by malicious software?

Malicious software is software that is intentionally included or inserted in a system for a harmful purpose. They are classified in to two categories: those that need a host program and those that are independent.

14. Define virus?

A virus is a piece of software that can infect other programs by modifying them; the modification includes a copy of the virus program, which can then go on to infect other programs.

15. Define a worm?

A worm is a program that can replicate itself and send copies from computer to computer across network connections. Upon arrival, the worm may be activated to replicate and propagate again. In addition to propagation, the worm usually performs some unwanted functions.

16. Name some malicious software's?

Key categories of malicious software are:

1. Backdoor: (Trap door) is a secret entry point in to a program that allows someone that is aware of the backdoor to gain access without going through the usual security access procedures.
2. Logic bomb: is a code embedded in some legitimate program that is set to explode when certain conditions are met.
3. Trojan horses: is a useful, program or command procedure containing hidden code that, when invoked, performs some unwanted or harmful function.
4. Zombie: A zombie is a program that secretly takes over another internet attached computer and then uses that computer to launch attacks that are difficult to trace to the zombie's creator.

17. Name the four phases of the lifetime of a virus?

A typical virus goes through the following four phases:

1. Dormant phase
2. propagation phase
3. Triggering phase
4. Execution phase

18. Name the different types of viruses?

The most significant types of viruses are:

1. Parasitic virus
2. Memory-resident virus
3. Boot sector virus
4. Stealth virus
5. polymorphic virus
6. metamorphic virus
7. macro virus
8. E-mail viruses

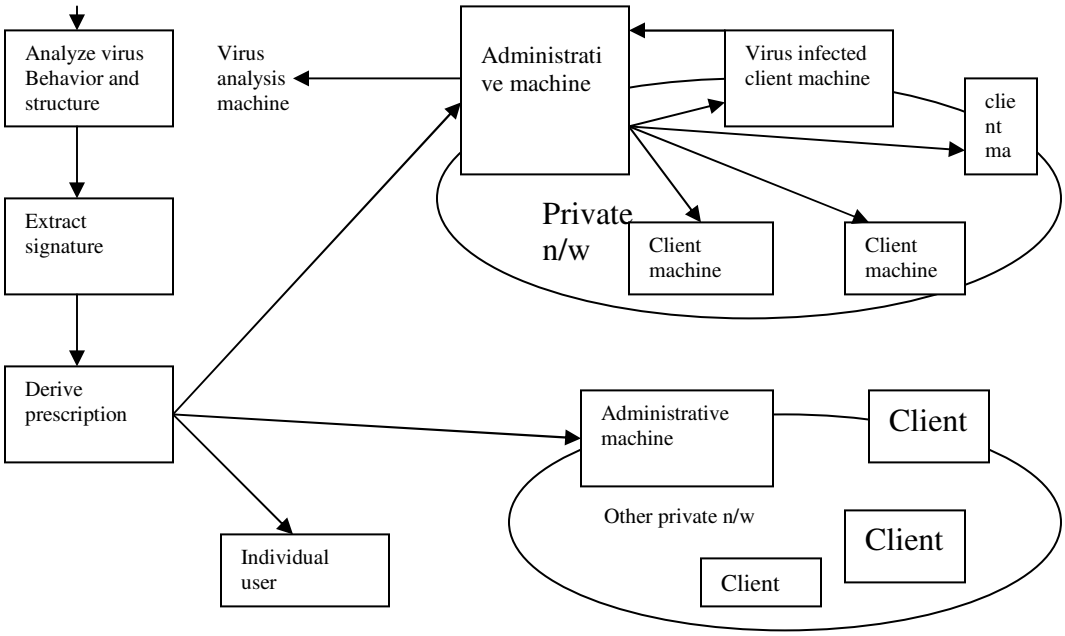
19. Name the state of art in worm technology?

The state of art in the worm technology includes the following:

1. Multiplatform
2. multiexploit
3. ultrafast spreading

4. polymorphic
5. metamorphic
6. transport vehicles
7. zero-day exploit

20. Diagrammatically illustrate a digital immune system?



21. Define a firewall?

A firewall forms a barrier through which the traffic going in each direction must pass. A firewall security policy dictates which traffic is authorized to pass in each direction. A firewall may be designed to operate as a filter at the level of IP packets, or may operate at higher protocol layer.

22. What are the design goals of firewall?

The design goals of firewall are:

1. All traffic from inside to outside, and vice versa, must pass through the firewall.
2. Only authorized traffic, as defined by the local security policy. Will be allowed to pass.
3. The firewall itself is immune to penetration.

23. What are the advantages of firewall?

The advantage of firewall are the following:

1. A firewall defines a single choke point that keeps unauthorized users out of the protected network.
2. A firewall provides a location for monitoring security-related events.

3. A firewall is a convenient platform for several internet functions that are not security related.
4. A firewall can serve as a platform for IPSec.

24. What are the limitations of firewalls?

The limitations of the firewalls are:

1. The firewall cannot protect against attacks that bypass the firewall.
2. The firewall does not protect against internal threats.
3. The firewall cannot protect against the transfer of virus-infected programs or files.

25. What are the types of firewalls used?

The common types of firewalls used are:

1. Packet-filtering router
2. Stateful Inspection firewalls
3. Application-level gateway
4. Circuit-level gateway
5. Bastion host

26. Define a trusted system?

A trusted system is a computer and operating system that can be verified to implement a given security policy. Typically, the focus of a trusted system is access control. A policy is implemented that dictates what objects may be accessed by what subjects.

Part B

1. Define intrusion and the methods used for intrusion detection?
2. Explain password management?
3. Define malicious software and the different kinds of malicious software's?
4. Explain viruses and related threats?
5. Explain the virus counter measures that are employed?
6. Explain firewall and their design principles?
7. Explain trusted systems?