Department of Computer Science and Engineering
CS6004 - Cyber Forensics
Question Bank (2017-18 ODD)

Unit 2. E-MAIL SECURITY & FIREWALLS

Part A

1. What are the security services provided by PGP ?

PGP uses a combination of symmetric secret-key and asymmetric public-key encryption to provide security services for electronic mail and data files. It also provides data integrity services for messages and data files by using digital signature, encryption, compression (zip) and radix-64 conversion.

2. List the various compression used in PGP?

- ZIP algorithm
- LZSS compressor
- LZFG compressor
- Huffman compression

3. Consider a packet with length 100. Compute its length encoded in one octet.

100 (decimal) = 01100100(binary)

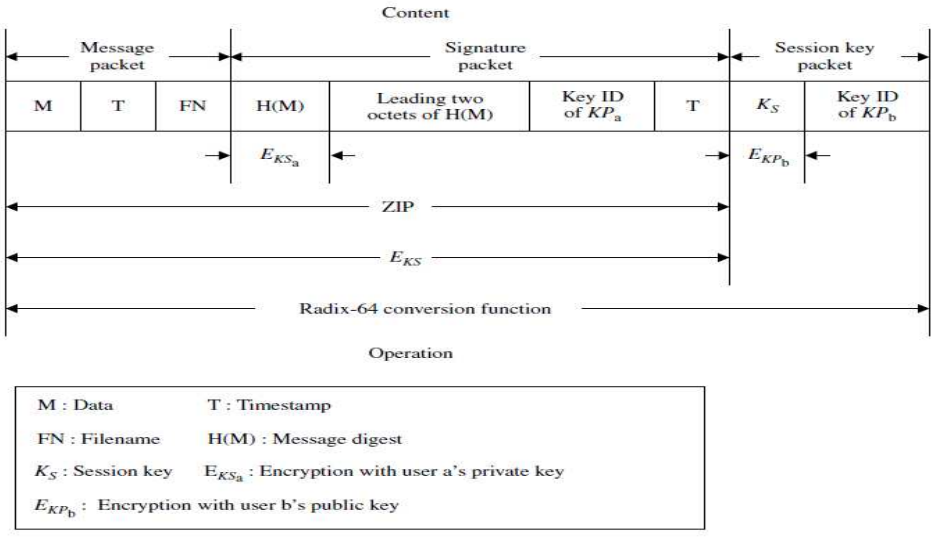
$= 2^6 + 2^5 + 2^2$

= 0x64 (hex)

Thus, a packet with length 100 may have its length encoded in one octet: 0x64. This

header is followed by 100 octets of data.

4. Draw the PGP message format.



5. What are the security services provided by S/MIME ?

S/MIME provides the following cryptographic security services for electronic messaging applications:

- Authentiaction
- Message integrity
- Non-repudiation of origin (using digital signatures)
- Privacy
- Data security (using encryption)

6. What are the disadvantages of SMTP ?

- SMTP lacks certain types of functions.

- SMTP lacks the security specified in X.400.

- Its simplicity limits its usefulness.

7. Consider an MIME message that contains a photograph in standard GIF representation. Write the header format of this message.

The header will contain the following :

MIME header
MIME Version: 1.1
Content Type: Image/GIF
Content Transfer Encoding: Base64

Optional headers:

- Content-Description
- Content-Disposition

8. What is triple wrapped message ?

A triple wrapped message is one that has been signed, then encrypted and then signed again. The signers of the inner and outer signatures may be different entities or the same entity. The S/MIME specification does not limit the number of nested encapsulations, so there may be more than three wrappings.

9. What is Firewall?

A firewall is a device or group of devices that controls access between networks. It is a security gateway that controls access between the public Internet and an intranet (a private internal network) and is a secure computer system placed between a trusted network and an untrusted internet. The aim of this wall is to protect the intranet from Internet-based attacks.

10. Name the Categories of firewall

Firewalls are classified into three common types:

- packet filters
- circuit-level gateways
- application-level gateways

11. What are the advantages and disadvantages of firewall?

Advantages:

- The firewall imposes restrictions on packets entering or leaving the private network. All traffic from inside to outside, and vice versa, must pass through the firewall, but only authorised traffic will be allowed to pass. Packets are not allowed through unless they conform to a filtering specification.
- Firewalls create checkpoints (or choke points) between an internal private network and an untrusted Internet

Disadvantages:

- It cannot protect against internal
- Threats such as an employee who cooperates with an external attacker.
- It is also unable to protect against the transfer of virus-infected programs or files because it is impossible for it to scan all incoming files, e-mail and messages for viruses

12. How will the firewall helps the user 'A' in a trusted network to connect to the Internet?

A firewall is a network security system, either hardware- or software-based, that uses rules to control incoming and outgoing network traffic.A firewall acts as a barrier between a trusted network and and an untrusted network. A firewall controls access to the resources of a network through a positive control model. This means that the only traffic allowed onto the network is defined in the firewall policy; all other traffic is denied.

13. When will the firewall block the connection from the Internet?

Firewalls are programmed in a definite manner and hence they can filter data based on destination and source IP address. IP addresses are unique numbers that can identify the location of a single host. Traffic filtering based on IP address denies information based on network/computers. The prime benefits of filtering information based on destination and source IP address are as enlisted below:

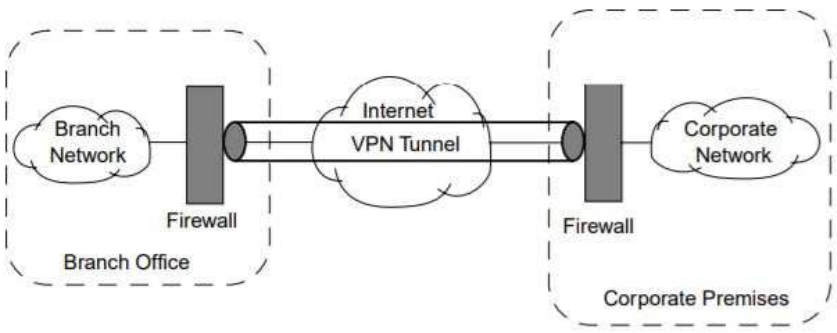
- Possible to Configure Firewalls Meant to Block Certain Websites
- Promotes a Type of Destination Filtering
- Facilitates Administrators to Disallow Instant Messaging

14. List the attacks from which the firewall protects the Trusted Network.

The firewall provides protection from various kinds of IP spoofing and routing attacks

15. Can we implement a VPN in firewall

Using the tunnel mode capability, the firewall can be used to implement Virtual Private Networks (VPNs). A VPN encapsulates all the encrypted data within an IP packet.



16. What tool is used to detect Intruder attack?

There are a wide variety of IDSs available, ranging from antivirus to hierarchical systems, which monitor network traffic. The most common ones are listed below.

- NIDS (Network intrusion detection systems)
- HIDS (Host intrusion detection systems)
- Signature based IDS
- Anomaly based IDS
- Passive IDS
- Reactive IDS

17. How will SOCKS establish a connection between a trusted network and un-trusted network?

- When a TCP-based client wishes to establish a connection to an object that is reachable only via a firewall, it must open a TCP connection to the appropriate SOCKS port on the SOCKS server system. The SOCKS service is conventionally located at TCP port 1080.
- If the connection request succeeds, the client enters negotiation for the authentication method to be used, authenticates with the chosen method, and then sends a relay request.
- The SOCKS server evaluates the request, and either establishes the appropriate connection or denies it.

18. How the choke point helps the firewall device to prevent the hacker?

- A choke point is the point at which a public internet can access the internal network. Since all traffic is flowing through the firewalls, security administrators, as a firewall strategy, need to create choke points to limit external access to their networks.
- Once these choke points have been clearly established, the firewall devices can monitor, filter and verify all inbound and outbound traffic. Since a choke point is installed at the firewall, a prospective hacker will go through the choke point.
- If the most comprehensive logging devices are installed in the firewall itself, all hacker activities can be captured. Hence, this will detect exactly what a hacker is doing

19. What is DMZ?

De-militarised Zone (DMZ) The DMZ is an expression that originates from the Korean War. It meant a strip of land forcibly kept clear of enemy soldiers. In terms of a firewall, the DMZ is a network that lies between an internal private network and the external public network. DMZ networks are sometimes called perimeter networks. A DMZ is used as an additional buffer to further separate the public network from the internal network

20. What is the need for logging and alarm in firewall?

- Logging and Alarms Logging is usually implemented at every device in the firewall, but these individual logs combine to become the entire record of user activity.
- Packet filters normally do not enable logging by default so as not to degrade performance. Since a choke point is installed at the firewall, a prospective hacker will go through the choke point. If so, the comprehensive logging devices will probably capture all hacker activities, including all user activities as well. The user can then tell exactly what a hacker is doing, and have such information available for audit. The audit log is an essential tool for detecting and terminating intruder attacks.

- Many firewalls allow the user to preconfigure responses to unacceptable activities. The firewall should alert the user by several means. The two most common actions are for the firewall to break the TCP/IP connection, or to have it automatically set off alarms.

21. What are the services provided by VPN?

- VPNs provide secure external access to internal resources.
- These are tunnelling protocols in the sense that their information packets or payloads are encapsulated or tunnelled into the network packets.
- All data transmitted over a VPN is encrypted to avoid eavesdropping of the data.
- Authentication, message integrity and encryption are very important fundamentals for implementing a VPN

22. What are the disadvantages of packet filters?

- It does not provide an error-correcting ability.
- They cannot discriminate between good and bad packets.
- Another weakness of packet filters is their susceptibility to spoofing. In IP spoofing, an attacker sends packets with an incorrect source address. When this happen, replies will be sent to the apparent source address, not to the attacker. This might seem to be a problem.

23. List the merits of circuit level gateways.

- The main advantage of a proxy server is its ability to provide Network Address Translation (NAT). NAT hides the internal IP address from the Internet.
- NAT is the primary advantage of circuit-level gateways and provides security administrators with great flexibility when developing an address scheme internally.
- If the packets do not violate any rules, the gateway sends out the same packets on behalf of the internal system. The packets that appear on the Internet originate from the IP address of the gateway's external port which is also the address that receives any replies. This process efficiently shields all internal information from the Internet.

24. List the merits of application level gateways?

- Application gateways (proxy servers) are used as intermediate devices when routing SMTP traffic to and from the internal network and the Internet.
- The main advantage of a proxy server is its ability to provide NAT for shielding the internal network from the Internet

25. What are the classifications of Proxies?

Proxies are classified into two basic forms:

• Circuit-level gateway

• Application-level gateway

Both circuit and application gateways create a complete break between the internal premises network and external Internet. This break allows the firewall system to examine everything before passing it into or out of the internal network.

26. Compare the single homed Bastion host with Dual homed Bastion host?

Single-homed bastion host: This is a device with only one network interface, normally used for an application-level gateway. The external router is configured to send all incoming data to the bastion host, and all internal clients are configured to send all outgoing data to the host. Accordingly, the host will test the data according to security guidelines.

Dual-homed bastion host: This is a firewall device with at least two network interfaces. Dual-homed bastion hosts serve as application-level gateways, and as packet filters and circuit-level gateways as well. The advantage of using such hosts is that they create a complete break between the external network and the internal network. This break forces all incoming and outgoing traffic to pass through the host. The dual homed bastion host will prevent a security break-in when a hacker tries to access internal devices

27. How the vulnerability issues are taken care in proxy server?

- Application proxies forward packets only when a connection has been established using some known protocol. When the connection closes, a firewall using application proxies rejects individual packets, even if they contain port numbers allowed by a rule set
- Each proxy is configured to allow access only to specific host systems.
- The audit log is an essential tool for detecting and terminating intruder attacks. Therefore, each proxy maintains detailed audit information by logging all traffic, each connection and the duration of each connection.
- Since a proxy module is a relatively small software package specifically designed for network security, it is easier to check such modules for security flaws.
- A proxy generally performs no disk access other than to read its initial configuration file. This makes it difficult for an intruder to install Trojan horse sniffers or other dangerous files on the bastion host.

28. Name the packet filters that provides security?

- TELNET packet filtering
- FTP packet filtering
- SMTP packet filtering

29. List the business requirement for SET.

The major business requirements for credit card transactions by means of secure payment processing over the Internet.

They are listed below:

1. Confidentiality of information (provide confidentiality of payment and order information)

2. Integrity of data (ensure the integrity of all transmitted data)

3. Cardholder account authentication (provide authentication that a cardholder is a legitimate customer of a branded payment card account)

4. Merchant authentication (provide authentication that a merchant can accept credit card transactions through its relationship with an acquiring financial institution

5. Security techniques (ensure the use of the best security practices and system design techniques to protect all legitimate parties in an electronic commerce transaction)

6. Creation of brand-new protocol (create a protocol that neither depends on transport security mechanisms nor prevents their use)

7. Interoperability (facilitate and encourage interoperability among software and network providers).

30. What are the system participants for SET protocol?

- Card holder
- Issuer
- Merchant
- Acquirer
- Payment gateway
- Certification authority

31. What cryptography principles are incorporated in SET protocol?

Cryptographic Operation Principles SET is the Internet transaction protocol providing security by ensuring confidentiality, data integrity, authentication of each party and validation of the participant's identity. To meet these requirements, SET incorporates the following cryptographic principles:

• Confidentiality.

• Integrity

• Authentication

32. What is Dual Signature?

SET introduced a new concept of digital signature called dual signatures. A dual signature is generated by creating the message digest of two messages: order digest and payment digest. The customer takes the hash codes (message digests) of both the order message and payment message by using the SHA-1 algorithm. These two hashes, ho and hp, are then concatenated and the hash code h of the result is taken. Finally, the customer encrypts (via RSA) the final hash code with his or her private key, Ksc, creating the dual signature. Computation of the dual signature (DS) is shown as follows:

DS = EKsc (h)

where h = H(H(OM)||H(PM))

= H(ho||hp)

EKsc (= dc) is the customer's private signature key.