s

SNS COLLEGE OF ENGINEERING

AN AUTONOMOUS INSTITUTION

Accredited by NAAC – UGC with 'A' Grade

Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

19EC625 – CYBER FORENSIC AND DATA SECURITY

UNIT II

E-MAIL SECURITY & FIREWALLS

PGP – S/MIME – Internet Firewalls for Trusted System: Roles of Firewalls - Firewall related terminology- Types of Firewalls – Firewall designs – SET for E-Commerce Transactions.

Part-A

1. What is application level gateway?

An application level gateway also called a proxy server; act as a relay of application-level traffic. The user contacts the gateway using a TCP/IP application,

such as Telnet or FTP, and the gateway asks the user for the name of the remote host to be accessed.

2. List the design goals of firewalls?

1. All traffic from inside to outside, and vise 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.

3. What is mean by SET? What are the features of SET?

Secure Electronic Transaction (SET) is an open encryption and security specification designed to protect credit card transaction on the internet. Features are:

1. Confidentiality of information

2. Integrity of data

3. Cardholder account authentication

4. Merchant authentication

4. What are the steps involved in SET Transaction?

1. The customer opens an account
2. The customer receives a certificate
3. Merchants have their own certificate
4. The customer places an order.
5. The merchant is verified.
6. The order and payment are sent.
7. The merchant requests payment authorization.
8. The merchant confirm the order.
9. The merchant provides the goods or services.
10. The merchant requests payment.

5. Define S/MIME?

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

6. What are the headers fields define in MIME?

MIME version. Content type.

Content transfer encoding. Content

id. Content description.

7. What is MIME content type and explain?

It is used to declare general type of data. Subtype define particular format for that type of the data. It has 7 content type & 15 subtypes. They are,

1. Text type Plain text. Enriched.
2. Multipart type

Multipart/mixed. Multipart/parallel. Multipart/alternative. Multipart/digest.

3. Message type

Message/RFC822. Message/partial. Message/external.

4. Image type

JPEG. CIF.

5. Video type.

6. Audio type.

7. Application type

Post script. Octet stream.

8. What are the key algorithms used in S/MIME?

1. Digital signature standards.
2. Diffi Hellman.
3. RSA algorithm.

9. Give the steps for preparing envelope data MIME?

1. Generate Ks.
2. Encrypt Ks using recipient' s public key. RSA algorithm used for encryption. Prepare the 'recipient info block' .
3. Encrypt the message using Ks.

10. What are the services provided by PGP services

- Digital signature Message encryption Compression
- E-mail compatibility
- Segmentation

11. Explain the reasons for using PGP?

a) It is available free worldwide in versions that run on a variety of platforms, including DOS/windows, UNIX, Macintosh and many more.

b) It is based on algorithms that have survived extensive public review and are considered extremely secure.

E.g.) RSA, DSS and Diffie-Hellman for public key encryption, CAST-128, IDEA, 3DES for conventional encryption, SHA-1for hash coding.

c) It has a wide range of applicability from corporations that wish to select and enforce a standardized scheme for encrypting files and communication.

d) It was not developed by nor is it controlled by any governmental or standards organization.

12. Why E-mail compatibility function in PGP needed?

Electronic mail systems only permit the use of blocks consisting of ASCII text. To accommodate this restriction PGP provides the service converting the row 8- bit binary stream to a stream of printable ASCII characters. The scheme used for this purpose is Radix-64 conversion.

13. Name any cryptographic keys used in PGP?

a) One-time session conventional keys. b) Public keys.

c) Private keys.

d) Pass phrase based conventional keys.

14. What is meant by S/MIME? (A/M-12)

S/MIME (Secure/Multipurpose Internet Mail Extensions) is a standard for public key encryption and signing of MIME data. S/MIME is on an IETF standards track and defined in a number of documents, most importantly RFCs (3369, 3370, 3850, 3851). S/MIME was originally developed by RSA Data Security Inc. The original specification used the IETF MIME specification with the de facto industry standard PKCS secure message format. Change control to S/MIME has since been vested in the IETF and the specification is now layered on cryptographic message syntax.

15. List out the types of firewalls.

1. Packet Filters
2. Circuit-Level Gateways
3. Application-Level Gateways

Part-B

1. Explain in detail about the PGP.
2. Explain in detail about the S/MIME.
3. Explain in detail about the Types of Firewalls in Internet Firewalls for Trusted

System.

4. Explain in detail about the Firewall related terminology in Internet Firewalls for Trusted System.

5. Explain in detail about the SET for E-Commerce Transactions.