DNSSEC and IPSEC

1. **What are the different ways a DNS hijack can be launched against a host? (2 Points)**

Ans: a) Infect the OS with a virus/trojan and update the DNS cache
b) Man in the middle attack
c) Response spoofing.

2. **What is the purpose of the additional section in the DNS response message? How could it be exploited by the attacker for DNS poisoning? (2 Points)**

Ans: The additional section in DNS response is used by a DNS server to provide additional information that may be requested by resolver later. This will reduce the time to resolve the name. The attacker can give spurious information in the additional information field that will be cached by the resolver leading to DNS poisoning.

3. **What are the issues with the current DNS mechanism that leads to security issues in DNS? (2M)**

Ans: DNS messages are shared in plain text, Uses UDP as transport protocol, The DNS information is distributed in the DNS hierarchy. End hosts rely on resolvers which are prone to attack, hijack.

4. **What are the new DNS records added while using DNSSEC? Explain what those records are for, in brief? (3M)**

Ans: a) DNSKEY: Contains the public key with associated parameters
b) RRSIG: Digital Signature of the RRSet with the associated parameters
c) DS: Delegation Signer contains the hash of the child's public key which is signed by the parent.

5. **Why does DNS use two keys ZSK and KSK instead of using only one key? (2M)**

Ans: Larger keys are preferred while creating the chain of trust. But smaller keys are preferred to sign the RRSet. So, DNS uses a larger KSK to create the chain of trust using DS records and uses a smaller ZSK to sign the RR.

6. **Why do DNS keys have to be updated using the Key Rollover mechanisms? What are the two mechanisms available for key rollover? (3M)**

Ans: In any cryptographic techniques, the keys should be used only for a limited amount of time. So the keys need to be updated by the DNS servers in the hierarchy (both KSK and ZSK).
The key rollover can be done either through pre-publish the new key or double signature methods.

7. **List out the scenarios where the Transport Mode and Tunnel Mode of IPSec will be used. (2M)**

Ans: Transport mode is used between two end hosts that need to use the IPSec for security. Tunnel mode is used between networks using IPSec Gateways.

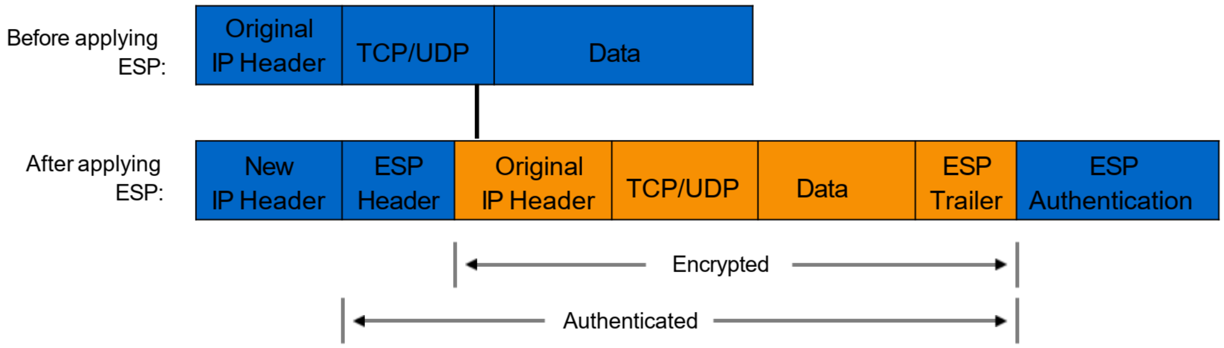
Transport mode : client to site VPN
Tunnel mode: Site to Site VPN

8. **While using AH in IPSec, what are the fields in the IP header that can't be authenticated and why? (2M)**

Ans: Some of the IP header fields are modified while the IP packet goes through multiple IP routers such as ToS, TTL, Checksum, Offset, Flags. So these fields can't be authenticated end to end.

9. **Provide the IP packet alteration in the case of ESP in Tunnel Mode. Specify which part of the packet is encrypted and which part of the packet is authenticated. (2M)**

Ans:



10. **In IPSec key exchange mechanism, there are two phases: IKE Phase 1 and IKE Phase 2. Both phases establish a security association between the endpoints. What is achieved in those two phases? (2)**

Ans: In Phase 1 a Security Association for management of IPSec is created. This can be used to establish the Security Association for multiple IPSec tunnels that can be created with different security levels.

In phase 1 of this process, IKE creates an authenticated, secure channel between the two IKE peers, called the *IKE security association*. The Diffie-Hellman key agreement is always performed in this phase.

In phase 2, IKE negotiates the IPSec security associations and generates the required key material for IPSec. The sender offers one or more transform sets that are used to specify an allowed combination of transforms with their respective settings. The sender also indicates the data flow to which the transform set is to be applied. The sender must offer at least one transform set. The receiver then sends back a single transform set, which indicates the mutually agreed-upon transforms and algorithms for this particular IPSec session. A new Diffie-Hellman agreement may be done in phase 2, or the keys may be derived from the phase 1 shared secret.

11. **What is Perfect Forward Secrecy (PFS)? What are the pros and cons of using PFS in creating IPSec? (2)**

Ans: PFS enables changing the Security Association in a periodic interval. Essentially changing the secret key periodically to minimize the impact when the key is compromised. PFS provides more security at the cost of establishing SA again and again.

12. **What are two possible ways a hijacked router can reroute internet traffic. (1 + 1 =2)**

Ans: (1) Advertise specific (or longest) IP prefix. (2) Advertise IP prefix owned by other networks.

13. **Which of the following statements are true: (1 point)**

a) DoS bug is a design flow attributed to protocol asymmetry with easy to send and difficult to generate response
b) DoS bug is a design flow attributed to protocol symmetry with easy to send and easy to generate response
c) DoS flood is associated with controlling a large number of machines to generate a large number of requests
d) DoS flood is associated with controlling a small number of machines to generate a large number of requests

Ans: a, c

14. What is the core problem in SYN flood attacks? What is the most effective way to defend SYN flood attacks? (1+1)

Ans: (1) Server commits resources (memory) before confirming client identity. (2) SYN Cookies.

15. In DNS amplification attack attacker sends DNS ___ request with spoofed source IP to open DNS resolvers. (1 point)

Ans) ANY

16. Which of the following statements are true about Mirai attack: (1 point)

a) Mirai botnet was successful because IoT security bar is very low
b) Exploited easy to guess IoT device default passwords
c) Only functions operated at L2/L3/L4 layers would be attacked, but not those at the application layer.

Ans) a, b

17. SSL/TLS renegotiation DoS can be mitigated by offloading _____ from CPU to SSL accelerator (1 point)

Ans) Encryption and Decryption

18. SlowLoris slow get attack can be defended by proxy server at ___. Proxy server waits for full header before forwarding to original server (1 point)

Ans) Edge

19. Hash DoS attack is successful when attacker manage to create ____ in hash table during insertion. (1 point)

Ans) Collisions

20. What is the purpose of SNI extension in TLS? How is it encrypted in TLS 1.3? 3 M

Ans: Server Name Indication (SNI) is used for virtual hostings i.e., multiple websites on the same IP address. Here Client Hello message carries client_hello_extension (SNI) which specifies domain name of the webserver.

Client uses Diffie-Hellman key exchange algorithm to generate a shared encryption key over an untrusted channel. The encrypted SNI encryption key is thus calculated on the client-side by using the server's public key (which is actually the public portion of a Diffie-Hellman semi-static key share, which is received by the client in a response to the DNS query over HTTPS (DoH)) and the private portion of an ephemeral Diffie-Hellman share generated by the client itself on the fly and discarded immediately after the ClientHello is sent to the server.

21. Name SIX web security guidelines and comment how they help in fixing various problems/attacks in using HTTPS for creating secure web applications? 9 M

Guideline	**Benefit**
Encrypt everything using HTTPS (TLS)	Confidentiality and Integrity
Deploy HSTS, HSTS preloading in browser	Prevents ssl_strip MITM attacks by enforcing client to connect over HTTPS always
Deploy CSP and upgrade insecure requests	Prevents Cross-site scripting (XSS) attacks and data injection attacks by preventing/restricing mixed content from 3rd party sites
HTTP Public Key Pinning	Prevents active and passive MITM attacks by letting a client caching public key of the site. Fake certs from hacked CAs won't cause any damage.
DNSSEC and DoT/DoH	Prevents DNS cache poisoning attacks and helps in improving privacy
DNS CA Authorization Records	Prevents active and passive MITM attacks by letting a site declaring CA that can sign its cert. Fake certs from hacked CAs won't cause any damage.
Certificate Transparency	Prevents active and passive MITM attacks by letting a client verify whether the cert is logged by CA in one or more log servers at the time of cert creation. Fake certs from hacked CAs won't cause any damage.

22. Integrating TLS with HTTP: Compare and contrast Pass-through (bypass) web proxy with Intercepting web proxy when a client visits https://iith.ac.in 6M

Pass-through (bypass) web proxy	**Intercepting web proxy**
2 TCP, 1 TLS and 1 HTTPS connections	2 TCP, 2 TLS and 2 HTTPS connections
Client uses HTTP CONNECT Method to request the proxy to establish a tunnel	Client uses HTTP CONNECT Method to request the proxy to establish a tunnel
Proxy relays TLS handshake messages between client and IITH web server by manipulating IP addresses and port Nos in both the directions.	Client needs to store the self-signed certificate of Proxy in the Trusted Root Store. Proxy issues bogus certificate on behalf of iith.ac.in when the client tries to setup TLS handshake to iith website
More secure, no privacy issues like in case of intercepting proxy	Less secure, privacy issues
No caching benefits	Caching benefits when multiple clients try to visit the same website

23. DNSSEC, DNS over TLS (DoT), DNS over HTTPS (DoH) standards are meant for improving security and privacy of DNS traffic. Take an example of public resolvers like Google Public DNS and explain how these standards play a role in improving security and privacy of DNS traffic. Are these standards complimentary with each other? How is the adoption of these standards? Are there any side effects when you choose to use a public resolver over the resolver of your ISP? (6M)

DoH and DoT enhance privacy and security between clients and resolvers, complementing Google Public DNS validation of DNSSEC to provide end-to-end authenticated DNS for DNSSEC-signed domains. Between DoH and DoT, DoH is more popular as browser vendors started implementing it where as DoT requires OS vendors to play a role, which is not happening. DoT and DoH are same except in usage of port nos and HTTP methods. Since the link b/w client and resolver is protected when DoT/DoH is used, it offers more security and privacy (local ISP, govts do not have any clue on which sites you are visiting and URL based firewall/censoring won’t work). Compared to local resolvers, public resolvers do a better job of DNSSEC validations.

DoT/DoH are complementary to DNSSEC. In general the adoption of these standards is low as Internet is a fully distributed system with so many players with different objectives. If not implemented properly, DNSSEC can lead to failure of resolutions altogether.

Side effect: DNS traffic of the entire world is now going to a handful of companies. Though these companies have stringent privacy laws, when it comes to national security, they may provide backdoor access to law enforcement agencies in the countries of their operation. ISPs do not get any visibility into what is happening in their pipes. When a malware is spreading like a fire, they may n’t able to take any actions to contain it quickly.

https://developers.google.com/speed/public-dns/docs/secure-transports

https://hacks.mozilla.org/2018/05/a-cartoon-intro-to-dns-over-https/