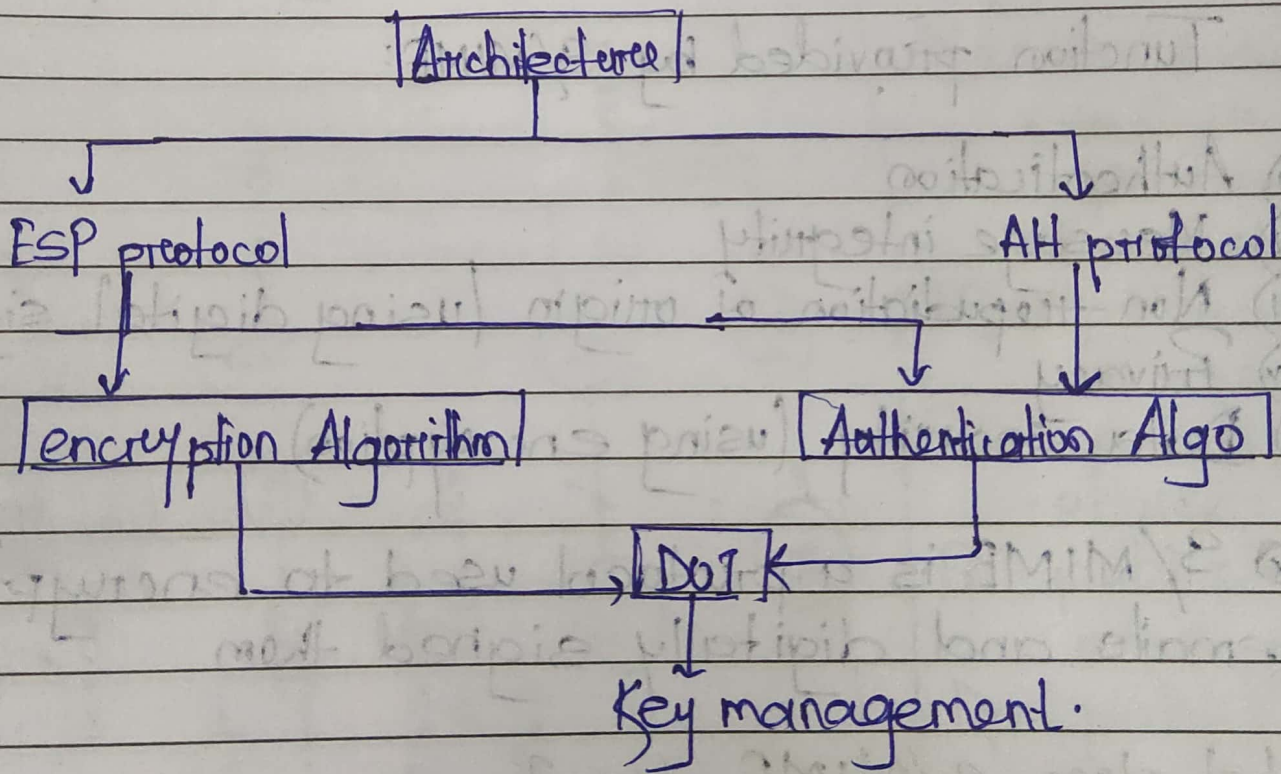
PAGE:

IP Security: It is a framework for protecting communication over IP.

1) Architecture:
⇒ It uses two protocols to secure the traffic on data flows. They are
= ESP (Encapsulation Security Payload)
= AH (Authentication Header).

⇒ It includes protocols, algorithms, Domain of interpretation and key management.
⇒ provides confidentiality, authentication and integrity.

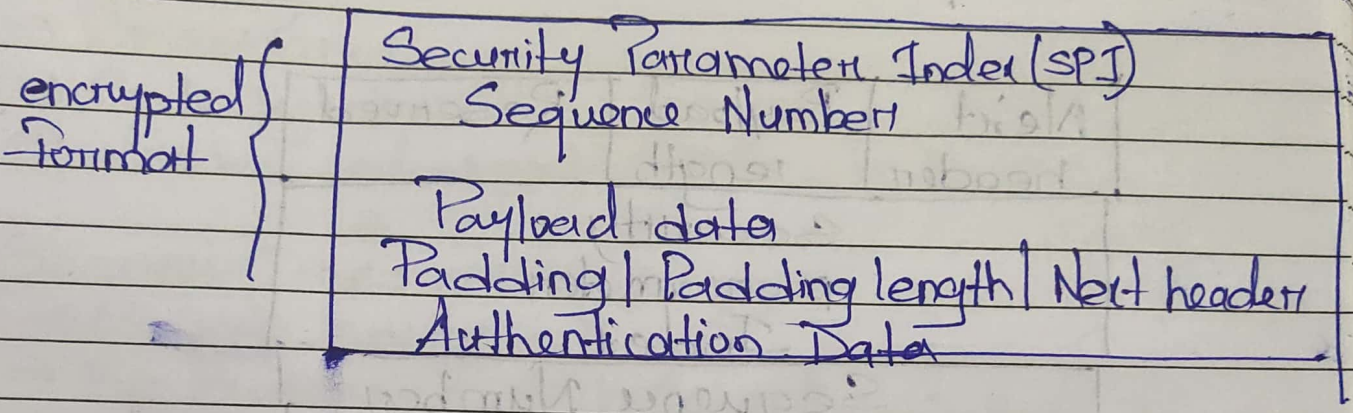


Architecture covers the general concepts definations, protocols, algo and security requirements of IP security technology.

ESP protocol:

⇒ Provides a confidentiality service.
⇒ Implemented either two ways -
a) ESP with optional authentication
b) ESP with Authentication

Packet format ⇒



Security Parameter Index (SPI): Used by security association to give unique number to the connection built between the client and server.

Sequence number: Are alloted to every packet so that on the receiver side packets can be arranged properly.

Payload Data: It's an actual data that are in encrypted form for confidentiality purpose.

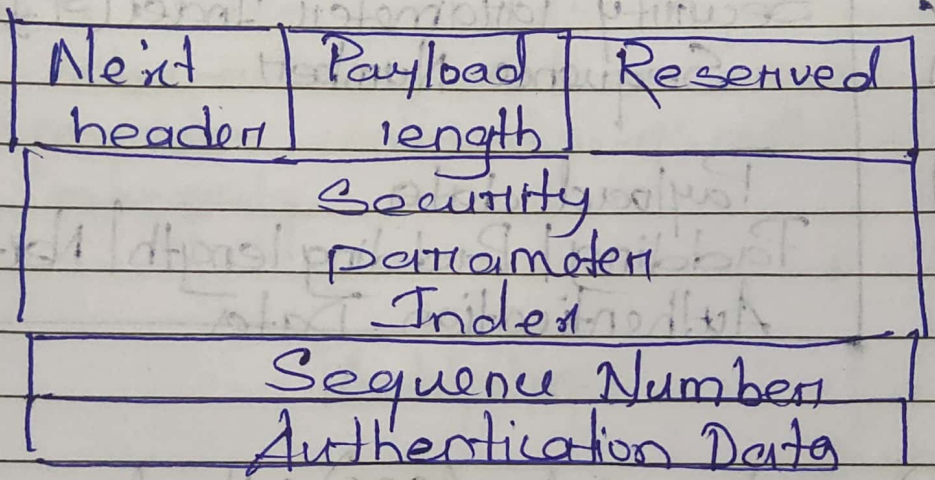
Padding: Extra bits of space are added to the original message in order to ensure confidentiality.

Good Write

Authentication data: Optional field in ESP packet format.

☞ Authentication header: Provides authentication and integrity service.

Implemented as authentication with Integrity.



It covers the packet format and general issue related to the use of AH for packet authentication of integrity.

Authentication Algorithm: Contains the set of documents that describe the authentication algorithm used for AH for the authentication option of ESP.

—o—

DATE: __/__/____
PAGE: _____

Web security ⇒ Web security refers to the protective measures and protocols that organization adopt to protect the organization from cyber criminals and threats that use the web channel.

Top web security threats:
⇒ Cross-site scripting (XSS)
⇒ SQL injection
⇒ Phishing
⇒ Ransomance
⇒ Code Injection
⇒ Viruses and worms

Security measures:
⇒ Update softwares.
⇒ Be aware of SQL Injection
⇒ Cross-site scripting (XSS)
⇒ Error messages
⇒ Data validations
⇒ password.

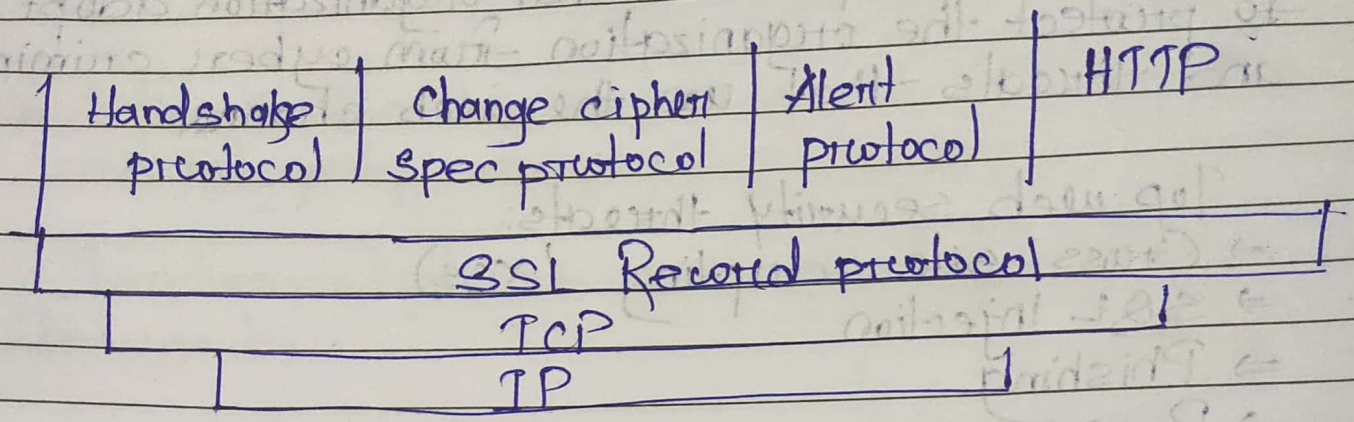
Secure Socket Layer (SSL): SSL provides security to the data that is transferred between web browsers and web servers.

It encrypts the link between a web server and browsers and which ensures that all data passed between them remain private and face from attack.

→ lies between application layer and transport layer of TCP/IP.

Good Write

SSL protocol stack:



SSL Record Protocol: (Confidentiality and Integrity)
It has two services
i) Confidentiality (done by encryption)
ii) Message integrity (done by MAC).

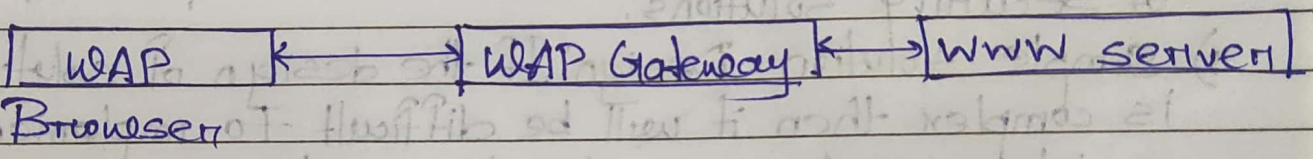
Working: Application data is divided into fragments. The fragments is compressed and the encrypted MAC (Message Authentication Code) generated by SHA algo. and MD5 is appended. At last SSL header is appended to the data.

DATE: __/__/____
PAGE: _____

WAP security: It is a specification for a set of communication protocols to standardize the way wireless devices such as mobile phones and radio transceivers can be used for internet access including email, the web, newsgroups and instant messaging.

Wireless Markup Language was used to create pages that can be delivered using WAP.

WAP Architecture:



WAP model and layers:

Similar to client-server model but uses an additional WAP gateway as an intermediary between client and server.

WAP protocol stack

Wireless session protocol
Wireless transaction protocol.
Wireless transport layer security
Wireless datagram protocol.

Use of WAP:

⇒ Wireless networks and mobile phone operators
⇒ Content providers.
⇒ end users.

Firewall design principles:

A firewall is a hardware or software to prevent a private computer or networks of computers from unauthorized access, it acts as a filter to avoid unauthorized users from accessing private computers and networks.

Principles:

i) Developing security policy: Without it, there is increase in risk as there will not be a proper implementation of security solutions.

ii) Simple solution Design: If the design of solution is complex then it will be difficult to implement, maintain and upgrades by analysing new possible threats, efficiency keeping in mind yet simple in struct.

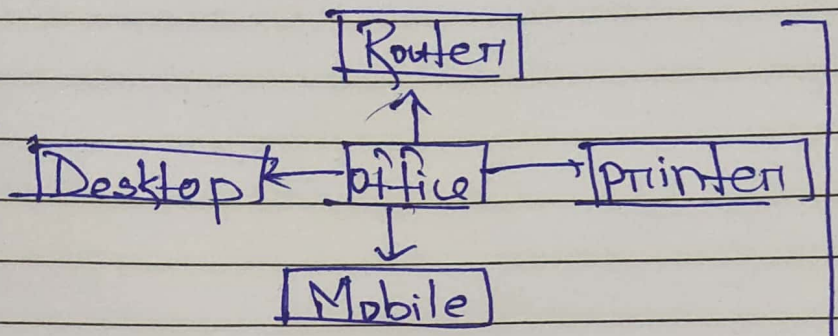
iii) Choosing right device: If the outdated devices is used for designing firewall, it exposes the network to risk & is almost useless.

iv) Layered defence: A network defence must be multi-layered because it gives an edge to the security design and finally neutralize the attacks on the system.

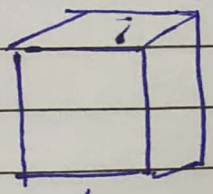
v) Consider Internal threats: Sometimes internal threats is neglected which makes the network weaker and vulnerable, filtering them adds a new layer in security point of view.

Virtual private network security: It is a way to extend a private network using network such as internet.

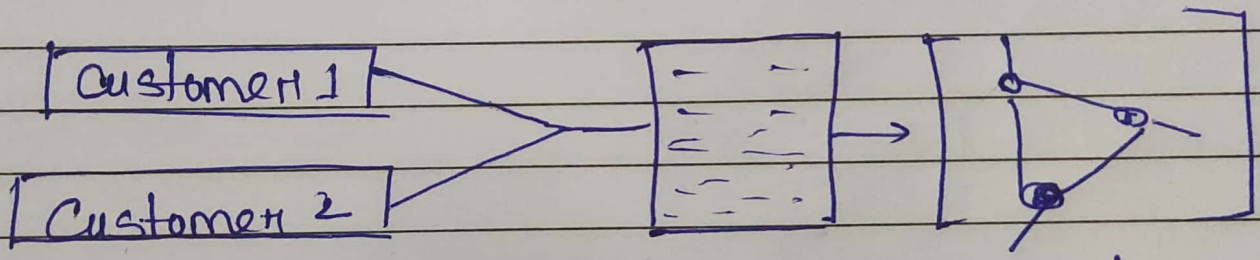
(i).



VPN server.



(ii)



—x—