* Assignment - 3 *

1) Difference between kerberos version 4 & version 5. ?

Basis of Comparisions	Kerberos version 4	Kerberos version 5
year of release.	Kerberos V4 was released in 1980's before V5 was released	The Kerberos V4 was Published in 1993, 13 year after the release of kerberos version 4.
Principal name	Kerberos V4 uses the Principle name Partially	Kerberos V5 uses the entire principal name
encryption techniques	Kerberos V4 uses DES encryption techniques	In Kerberos V5, the cipher text is tagged with an encryption type identifier and therefore type of encryption can be used.
encoding	Kerberos V4 uses the receiver makes right enloding system.	The Kerberos V5 uses the ASN.1 coding system.
Ticket lifetime	In kerberos V4 the ticket life time has to be specified in units of 5 minutes	In kerberos V5, ticket one life time can specify an explicit start and finish times allowing arbitary life times

Ticket support.	Ticket support is satisfactory in this version.	Ticket support is well extended. facilitates forwarding. renewing & post dating tickets.
IP address.	Kerberos V4 contains only a few IP address and other address for types of n/w protocol.	Kerberos V5 contains multiple IP address for types of n/w protocols
Key	Given that the same key is used repeatedly to gain a service from particular server there is a risk that an. attacker can replay msg from an old session to the client or server	In kerberos versions this is avoided by requiring a sub session key which is used only for one connection.

2) Key management in IP security ~~ex~~ OAKLEY protocol?, Key ~~tra~~

Key management:

The IPsec Architecture document mandates support for two types of key management.

Manual:

A system administrator manually configures each system with its own key and with the keys of other communicating systems. This

is practical for small relatively static environ-
-ment.

Automated:

An automated system enables the on demand creation of keys for SAs and facilitates the use of keys in a large distributed system with an evolving configuration.

The key management protocol for IPsec is referred to as ISAKMP/OAKley.

OAKley key determination protocol:

OAKley is a key exchange protocol based on the diffie-Hellman algorithm. OAKley is generic is that it doesn't dictate specific formats

⇒ OAKley is the specific key exchange algorithm mandated for use with the initial version of ISAKMP.

⇒ It is based on diffie-Hellman.

* A & B agree on 2 global parameters q & α
* A selects a random integer x_a as its private key, & transmit to B its public key

$$Y_a = \alpha^{x_a} \bmod q.$$

* B also same as A so $Y_b = \alpha^{X_b} \bmod q$

⇒ shared version key for users A & B is K_{AB}:

$$K_{AB} = \alpha^{X_a \cdot X_b} \bmod q.$$

⇒ diffie-Hellman is subject to a man-in the middle attack.

⇒ It doesnt provide any information about the indenties of the parties.

⇒ OAKley overcomes these 2 limitations.

<u>Uses:-</u>

1) It employs a mechanism known as cookies to clogging attacks.

2) It enables the 2 parties to negotiate a group.

3) It uses nonces to ensure against replay attack.

4) It enables the exchange of deffie-Hellman public key values.

5) It authenticates the deffie-Hellman exchange to man in the middle attacks.

⇒ Three different authentication methods can be used with oakley:

- Digital signatures
- Public-key encryption

- symmetric - key encryption.

⇒ The cookie exchange requires that each side send a pseudo random number, the cookie in the initial message, which the other side acknowledges.

⇒ The key management protocol for IPSEC is referred to as ISAKMP / OAKLEY.

⇒ This acknowledgement must be repeated in the first message of the diffie - Hellman key exchange If the source address was forged, the opponent gets no answer.

⇒ Thus an opponent can only force a user to generate acknowledgements and don't perform the diffie - Hellman calculation.