Kerberos Problem
Ticket granting ticket is issued by TGS to users. Each time the user requires access to new service, the client applies to the TGS, using the ticket granting ticket to authenticate itself.
Ticket(tgs) = Ektgs[IDc || ADc || IDtgs || TS1 || Lifetime1].

14.8 X.509 defines a framework for the provision of authentication services by the X.500 directory to its users. The directory may serve as a repository of public-key certificates. Each certificate contains the public key of a user and is signed with the private key of a trusted certification authority. In addition, X.509 defines alternative authentication protocols based on the use of public-key certificates.

14.9 A chain of certificates consists of a sequence of certificates created by different certification authorities (CAs) in which each successive certificate is a certificate by one CA that certifies the public key of the next CA in the chain.

15.7 PGP includes a facility for assigning a level of trust to individual signers and to keys.

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

16.4 Transport mode provides protection primarily for upper-layer protocols. That is, transport mode protection extends to the payload of an IP packet. Tunnel mode provides protection to the entire IP packet.

16.7 Transport adjacency: Refers to applying more than one security protocol to the same IP packet, without invoking tunneling. This approach to combining AH and ESP allows for only one level of combination; further nesting yields no added benefit since the processing is performed at one IPSec instance: the (ultimate) destination. Iterated tunneling: Refers to the application of multiple layers of security protocols effected through IP tunneling. This approach allows for multiple levels of nesting, since each tunnel can originate or terminate at a different IPSec site along the path.

16.3 We show the results for IPv4; IPv6 is similar.