Hello Everyone! In this video, you will learn about security protocols PGP and Secure MIME, working on the application layer for, protecting emails.

Pretty Good Privacy is designed for securing email. It was developed by Phil Zimmermann. Earlier it was an open source product, but later it was converted into a low-cost commercial product. It provides privacy, integrity, authentication, and non-repudiation to emails. Integrity, authentication, and nonrepudiation Are provided with the help of digital signature, while confidentiality is ensured using asymmetric key encryption.

In PGP, raw attachment files are first encrypted with the public key of the receiver, before sending. On receiving, the attachment files are decrypted with the private key of the receiver.

PGP verifies the information of the sender, to ensure that the email was not intercepted by a third party.
All sensitive information is always protected. No one from the internet can view it and steal it. PGP ensures that the information which has been sent from the sender side has been received on the receiver side, without any change and no modification has been done in between. PGP ensures that the files once deleted, cannot be recovered later.

SMIME, secure/multipurpose internet mail extensions protocol is another email security mechanism. It is an email

signing security protocol that uses encryption to increase email confidentiality and integrity. It uses public key encryption to secure emails.

Like PGP, S/MIME also uses public key encryption to encrypt emails. The figure explains the process clearly. At sender side the receiver's public key is used to encrypt while at the receiver side, the receiver's private key is used to decrypt.

Let's Understand the difference between Pretty Good Privacy (PGP) and S/MIME protocols.

PGP is an open source software package that is designed for securing emails. Phil Zimmerman developed it. This protocol takes multiple steps to secure the email. These steps include encryption, ensuring Authentication, Compression, Segmentation, Reassembly. Whereas, S/MIME is a security-enhanced version of Multipurpose Internet Mail Extension (MIME). This protocol also uses public key cryptography for digital sign, encrypt or decrypt the email. User acquires a public-private key pair from a trusted authority and then makes appropriate use of those keys with email applications.

PGP is designed for securing plain text emails. While S/MIME is designed to process emails with many multimedia files.

PGP depends on user key exchange validated by other users in a group. Whereas S/MIME relies on a hierarchically valid certificate for a key exchange, provided by a third party.

PGP is less costly as compared to S/MIME. While S/MIME is comparatively expensive.

PGP is good for personal as well as official use. While S/MIME is good for industrial use.

PGP recognizes X.509 certificates. It includes,
The PGP version number which identifies the version of PGP, The **certificate holder's public key, The certificate holder's information such as** "identity" of the user, It also includes The **digital signature of the certificate owner —** also called a *self-signature,* **The certificate's validity period which defining the** certificate's start date/ time and expiration date/ time; **The preferred symmetric encryption algorithm for the key —** indicating the encryption algorithm to which the certificate owner prefers to have information encrypted. The supported algorithms for encryption are are CAST, IDEA, or Triple-DES.
S/MIME is derived from the PKCS#7 data format for the messages and the X.509v3 format for certificates.

Thank You.