CS381 Exercise 13

Name: Zhang Yupeng

Student ID: 5130309468

2. Describe the similarities and differences between PGP and S/MIME.

S/MIME and PGP are both protocols used for authentication and privacy to messages over the internet.

PGP, stands for Pretty Good Privacy, is a data encryption and decryption computer program that offers cryptographic privacy and authentication for Internet data transmission. PGP is widely used for signing, encrypting and decrypting electronic data to maximize the security issues of data exchange. The protocol S/MIME refers to Secure/Multipurpose Internet Mail Extensions.

S/MIME is recently included in the latest versions of the web browsers from renowned software companies like Microsoft and Netscape and has also been broadly accepted by many vendors in all around the world. It is also driven as a standard for public key encryption and signing of MIME data. S/MIME is based on an IETF standard and most commonly defined in RFCs documents. S/MIME provides the authentication, message integrity and non-repudiation of origin and data security services for electronic data transmission applications.

S/MIME is very closely similar to PGP and its predecessors. S/MIME is derived from the PKCS #7 data format for the messages, and the X.509v3 format for certificates. PGP encryption uses a serial combination of hashing, data compression, symmetric-key cryptography, and public-key cryptography.

While using PGP, one user has the ability to give directly a public key to another user or the second user can obtain the public key from the first user. PGP does not mandate a policy for creating trust and hence each user is free to decide the length of trust in the received keys. With the S/MIME, the sender or receiver does not rely on exchanging keys in advance and share a common certifier on which both can rely.

S/MIME is considered superior to PGP from an administrative perspective because of its strength, support for centralized key management through X.509 certificate servers and extensive industry support. PGP is more complicated from an end-user perspective, because it requires additional plug-ins or downloads to operate. S/MIME protocol allows most vendors to send and receive encrypted email without using additional software.

S/MIME is convenient because of secure transformation of all applications like spreadsheets, graphics, presentations, movies etc., but PGP was originated to address the security concerns of plain e-mail or text messages. S/MIME is also highly affordable in terms of its cost.

Summary:

S/MIME and PGP protocols use different formats for key exchange.

PGP depends upon each user's key exchange S/MIME uses hierarchically validated certifier for key exchange. PGP was developed to address the security issues of plain text messages. But S/MIME is designed to secure all kinds of attachments/data files.

Nowadays, S/MIME is known to dominate the secure electronic industry because it is incorporated into many commercial e-mail packages.

S/MIME products are cheaply available than for PGP.