Name: Devanshu Surana
Div: C Batch: C1
Roll No.: 23
Prn:1032210755

Lab A8: Demonstration of Email Security using – PGP or S/MIME for Confidentiality, Authenticity and Integrity

Objective of Lab

1. To understand how PGP provides a confidentiality and authentication service that can be used for electronic mail and file storage applications.
2. To understand and implement important services provided by PGP like Authentication (Sign/Verify), Confidentiality (Encryption/Decryption) , Compression, Email compatibility.

Theory

Both Pretty Good Privacy (PGP) and Secure/Multipurpose Internet Mail Extensions (S/MIME) are cryptographic protocols that provide confidentiality, authenticity, and integrity for email communication. However, they have some differences in terms of usage, implementation, and support. Let's briefly discuss each:

Confidentiality:

PGP uses hybrid encryption, combining symmetric and asymmetric encryption.
The message content is typically encrypted with a symmetric key, and this symmetric key is then encrypted with the recipient's public key.
This approach ensures confidentiality, as only the recipient with the corresponding private key can decrypt the symmetric key and then decrypt the message.

Authenticity:

PGP provides authenticity through digital signatures.
The sender signs the message with their private key, and the recipient can verify the signature using the sender's public key.
This ensures that the message was indeed sent by the claimed sender.

Integrity:

Integrity is maintained through the use of digital signatures.
Any alteration to the message will result in an invalid signature upon verification.

Usage:

PGP is often used for securing email communication, file encryption, and other secure messaging applications.
It's widely used for personal and non-corporate communication.
S/MIME (Secure/Multipurpose Internet Mail Extensions):
Confidentiality:

S/MIME also uses hybrid encryption.
The message content is encrypted with a symmetric key, and this key is encrypted with the recipient's public key.
Authenticity:

Similar to PGP, S/MIME uses digital signatures for authenticity.
The sender signs the message with their private key, and the recipient can verify the signature using the sender's public key.
Integrity:

Integrity is ensured through the use of digital signatures.
Any tampering with the message will result in an invalid signature during verification.
Usage:

S/MIME is often integrated into email clients and is commonly used in corporate environments.
It is well-suited for scenarios where users have digital certificates issued by a Certificate Authority (CA).
Considerations:
Interoperability:

PGP is more widely used in personal and non-corporate settings.
S/MIME is often preferred in corporate environments due to its integration with X.509 certificates.
Key Management:

PGP often relies on a decentralized "web of trust" model for key management.
S/MIME typically uses a hierarchical trust model with certificates issued by CAs.
Implementation:

PGP and S/MIME are implemented in various email clients and tools.
The choice between them may depend on factors such as user preferences, organizational policies, and existing infrastructure.

In summary, both PGP and S/MIME can provide confidentiality, authenticity, and integrity for email communication, and the choice between them may depend on factors like user preferences, organizational policies, and existing infrastructure.

Command Screen shots

Sending encrypted email with PGP is a four step process, consisting of the following steps:

1. Create the message that you want to send which can be done using some word processor.
2. Get the public key of the person to whom you are sending the message. One can get public key of a person either from the person himself or from any key server.
3. Ecrypt the message using the person's public key. It is done using the ea option. For example,
   $ pgp -ea <messagefile> <users public key id>
   encrypts the message in messagefile using user aldrin's key. The **a** is used to generate ASCII armored output.
4. Sending the encrypted message via your traditional electronic mail program.

$pgp -es <plaintext filename> <recipients_userid> [-u your_userid]
The -ka(key add) option adds new keys to a key ring.

Get the public key of the person you want to add to your public key ring (Getting others public key will be discussed later). Put it in some file. The command

$ pgp -ka filename

adds the key to your key ring. Try the -kv option to verify if its actually there. You can also specify the key ring to which you wish to add the key. For example the command

$ pgp -ka abc.asc

will add the public key stored in the file abc.asc into your key ring.

1.8 Removing keys from a key ring

The -kr (key remove) option removes keys from a key ring. For example-

$ pgp -kr aldrin arun.kr

would remove public key of user aldrin from the keyring. Typing

$ pgp -kr

would ask for the user to enter the name of the key to be removed. You can enter a user ID or the fragment of a user ID to select a key. PGP makes an intelligent selection from the keys

present and asks the user before deleting the key. You can also use the hexadecimal key ID to select a key.

Conclusion: Thus we have learned PGP or S/MIME for Confidentiality, Authenticity and Integrity.

FAQs:

1. Why you need PGP
2. What is Pretty Good Privacy (PGP) encryption?
3. How PGP encryption works
4. How end-to-end encryption works
5. What is PGP used for?

References: