Submitted By:

Name	Reg No	Email Address
Mirza Kashif Abrar	790604-T079	kasmir07 (at) student.hh.se
Abid Hussain	780927-T039	abihus07 (at) student.hh.se
Imran Ahmad Khan	770630-T053	imrakh07 (at) student.hh.se

Submitted To,

Yan Wan.

Introduction:

Pretty Good Privacy (PGP) it is software which is used for electronic privacy. It allows you to encrypt files and emails on the internet. It is used to encrypt the data and used to create the digital signatures. It converts the plaintext into cipher text. It is based on the public key cryptography for its effectiveness. Public key cryptography is a method in which users use *keys* to send and receive the secure documents. It generates two keys one pubic and private keys. Private Key is used to decrypt the message. It is freeware software for home users and at very low cost at commercial level.

Table of contents

Cryptography

Cryptography is the method in which mathematics technique is used to encrypt and decrypt the data (to convert the plaintext into cipher text).

Keys

It is a value which works in a cryptographic algorithm for the creation of cipher text from plain text. The size of key is measured in bits. The large size of key is more secure. PGP generate two files in hard disk for keys one for public key and one for private key, these files are know as key rings.

Digital Signature

It is used to verify the authenticity of the origin of data .It like a handwritten signature so that the sender can not deny that he/she has not sent the data. So it is a proof for the recipient.

Encryption and Decryption in PGP

In PGP the symmetric encryption algorithm CAST-128 is used. Alternatively IDEA(International Data Encryption Algorithm) or 3DES are also used. The 64-bit cipher feedback (CFB) mode is used.

CAST-128 is a block cipher used in a number of products, notably as the default cipher in some versions of GPG and PGP. In PGP each symmetric key is used only once. New key is generated as a random 128-bit number for each message, because it is used only once, the session key is bound to the message and transmitted with it. During this following steps are performed.

i. Sender creates a message and random 128-bit number is used ad session key only for this message.
ii. CAST-128 algorithm is used to encrypt the message.
iii. The session key is encrypted with RSA.
iv. The recipient use RSA with its private key to decrypt and recover the session key.
v. The session key is used to decrypt the message.

Five principal services provided by the PGP are:

Authentication

The sender creates a message. SHA-1 is used to generate 160 bit hash.
SHA-1 generated hash is encrypted with RSA using the sender's private key, and pretended to message. The receiver uses RSA with the sender's public key to decrypt and recover the hash code. The receiver generates the SHA-1 from the message received, and compares it with the decrypted one.

Confidentiality

Sender creates a message and random 128-bit number is used ad session key only for this message.CAST-128 algorithm is used to encrypt the message. The session key is encrypted with RSA. The recipient use RSA with its private key to decrypt and recover the session key. The session key is used to decrypt the message.

Compression

The compression algorithm used in PGP. PGP first signs the document and then compresses it. Encryption is done after compression, thus making the message containing less redundant information. The compression issue is also because of compatibility. These way different versions of PGP can use different versions of compression algorithm but there is always compatibility.

Email compatibility

When the plaintext is encrypted, the e-mail body consists of a stream of arbitrary 8-bit octets. Because many e-mail systems only permit the use of blocks consisting of ASCII text, PGP encodes the resulting message from raw 8-bit to ASCII text. To accommodate this is using radix-64 conversion. Thus the receiving end will convert the message from base-64 to raw 8-bit before performing further processing

Segmentation

We know that the PGP is used to secure the internet communication and to protect the data from hacking or misuse. The email message or data on the internet have large files. The PGP has the facility to automatically make the blocks of data and create encrypted message into segmentation according to the appropriate length. On the recipient the message or data reassembled before decryption procedure start.

A signing is an event at which people present their PGP-compatible keys to others in person, who, if they are confident the key actually belongs to the person who claims it, digitally sign the PGP certificate containing that public key and the person's name, etc. This is one way to strengthen the web of trust. The following steps are performed in signing the message.

i. PGP retrieves the senders private key from the private key ring using your userid as index. If userid not provided in the command the first key on the ring is retrieved.
ii. PGP prompts the user for passphrase to recover the encrypted private key.
iii. The signature component of the message is constructed.

SDA (Self Decrypting Archive)

A self decryption archive (SDA) is self decryption executable file that is easy way to encrypt your file with your passphrase and also you can send this file to other person. It is also secure exchange file method between authenticate members because SDA require passphrase to encrypt and decrypt file. Member should know passphrase and in this method one advantage is that no PGP require on other member system. He or she can receive secure file or message from one side PGP installed software member.

PGP Disk

PGP provide one more security that is called PGP disk. It is easy to use encryption application. PGP disk provide hard disk security that you can secure your secret data in encrypted virtual hard disk. In this method you can create a virtual disk by some encryption Algorithm. It generate a encrypted disk with your secure passphrase.

Although it's a single file, PGPdisk acts very much like a hard diskin that it provides storage space for your file and application. You can think it just like your usb or an external hard disk. To use the applications and files stored in the volume, you can mount it or make it accessible to you. When a PGPdisk volume is mounted, you can use it as you would use any other disk. You can install applications within the volume or move or save your files to the volume. When the volume is unmounted it is inaccessible to anyone who does not know your secret passphrase. Even a mounted volume is protected. It is stored in encrypted format unless a file or application is in use. If your computer should crash while a volume is mounted, the volume's contents remain encrypted and save its recoverable.

Conclusion

In this Project report we learned how to use PGP to encrypt our email message on the internet. Its providing good security by encryption method. This includes many technique to secure file like SDA , PGP disk and PGP encryption decryption technique . We know that email is the most used internet based application and It is widely used across all architectures and vendors platforms. So it is very helpful to protect our data and email messages on the internet.