Introducing PGP

Encryption to Secure Your E-mail

Michael Chesbro, Ph.D., CCIA, CCIP

February 8, 2014

PGP or "Pretty Good Privacy" is a data encryption program developed by Phil Zimmermann in 1991. Since its initial release PGP has undergone various upgrades and revisions, and over the years has become an "unofficial standard" for personal e-mail encryption. Both commercial and open source (freeware) versions of PGP are currently available. If you regularly communicate by e-mail, PGP can protect your private and personal messages from being read by anyone other than the intended recipient. If you have a business or organization that asks for public input via e-mail, having PGP set up and your PGP public key posted allows those who wish to do so to communicate with you securely. (It would be irresponsible for any organization to ask that private or sensitive information be sent via un-encrypted e-mail, or even worse through social media, such as Facebook, Instagram, or Twitter.)

With PGP you have very strong encryption protecting your personal, private, and sensitive information. You also have the ability to digitally sign messages that you send to others so that the recipient can be confident that the information is in fact from you and hasn't been altered in any way. Some versions of PGP also support disk encryption and the creation of self-decrypting archives. This paper focuses on the obtaining and using PGP for encrypting e-mail.

Where to Get PGP

PGP is available from several sources. The commercial version of PGP is owned by Symantec Corporation (http://www.symantec.com/encryption). The commercial version of PGP is likely the best choice for implementing PGP in a corporate or other large scale environment.

For personal use there are several freeware versions of PGP that should easily meet your needs. GNU Privacy Guard (http://www.gnupg.org/) is perhaps the most commonly used freeware implementation of PGP. GNU Privacy Guard has a version for Windows (GPG4WIN http://www.gpg4win.org/) and a version of MAC-OS (GPGMail https://gpgtools.org). Mailvelope (http://www.mailvelope.com/) provides an open PGP implementation for web based e-mail. Mailvelope works as a Google Chrome extension or as a Mozilla Firefox add-on. Mailvelope comes pre-configured to work with Gmail, GMX, Outlook.com, and Yahoo! Mail, and is easily configurable for other platforms. Portable PGP (http://ppgp.sourceforge.net/) runs from a USB / Thumb Drive, and is a JAVA based version of PGP that works on both Windows and Linux platforms. PGP integrates with Hushmail (https://www.hushmail.com), a web-based secure e-mail service. PGP is also available for your cell-phone: PGP for iOS

(http://ipgmail.com/) and Android Privacy Guard (APG) (https://code.google.com/p/android-privacy-guard/). Older implementations of PGP can be found on the International PGP Homepage (http://www.pgpi.org/).

Regardless of which implementation of PGP you choose, the encryption is cross compatible with other current versions of PGP. This means that the commercial version of PGP will work with GNU Privacy Guard, and GNU Privacy Guard works with Mailvelope, and Portable PGP works with the commercial version of PGP, etc. Other functions of PGP (such as digital signatures) may not be supported in all implementations.

Using PGP

PGP uses public key (asymmetric) encryption, allowing the user to encrypt and sign digital content, such as e-mail. Once you have chosen a version of PGP that you want to use, you must generate a PGP Key Pair. PGP Key Pair generation is done by the PGP software installed on your computer. The PGP Key Pair consists of a public key that allows messages to be encrypted, and a private key that allows messages to be decrypted. As the key names suggest you give a copy of your PGP public key to everyone who might want to send you an encrypted message. You may even want to post your PGP public key to your web-page or upload it to a PGP public key server where everyone can find it and download a copy.

PGP Public Key Servers can be found at:

PGP Global Directory - https://keyserver.pgp.com/

MIT PGP Key Server - http://pgp.mit.edu/

University of Mainz (Germany) - http://pgp.uni-mainz.de/

Hushmail PGP Public Key Server - https://www.hushtools.com/hushtools2/index.php?

It is important to note that just because you obtained a PGP public key from a key server, there is no guarantee that the key belongs to the person you think it does. Be sure to match the e-mail address associated with the key with the e-mail address you are sending your message to. It is also important to confirm the PGP key fingerprint with the intended recipient of your e-mail to make sure you have the correct public key.

If you send an e-mail to more than one person you can encrypt the message with multiple public keys, thereby allowing each person with a corresponding private key to decrypt and read the message. You may also wish to encrypt e-mail that you send with your own public key so that you will be able to decrypt and read it after it has been sent.

Your PGP private key is used to decrypt messages encrypted with your corresponding public key. You must never share a copy of your private key with anyone. You should never post your

private key to the Internet, and of course you should never upload your private key to a PGP public key server.

Most of the current implementations of PGP are fairly simple to use. The best way to learn to use PGP is to install it on your computer and then practice exchanging encrypted messages with a friend who also uses PGP.

A message encrypted with PGP looks like this:

```
-----BEGIN PGP MESSAGE-----
Version: Mailvelope v0.7.0
Comment: Email security by Mailvelope - http://www.mailvelope.com

wcBMA8VP2M4MNOD5AQf8CbQvRaALDkznu7j/bq+EOx4HTS5+id5ZYwYXIEG2
hn8SWyBFnVpcbsay92ZNsTwanN0m8s7C1qYc5lgPlwpXc+4F3pEsC2oTHpfB
2qE24XjEIJN6w1+NYhnM4t8TnJuq3V2t1IBmHONxdguvQ1GsjaN3Yt7Xvnbo
KTK+zACffGwr2txvjkqt3bCaWbatdNaLq2SMkqAc8OABpSBXyluQwSlpHuGw
IpqxTYfdgZWk3HEFlpFv/k2A5mRcpwpbkQ71hYQInuDuVKMvz77ObOk7elmQ
1XYcCWKFIzYkWYwvpr4wFoFGR0shgii6qUKM0FYBc3kRn1Q8Z9rrbwM2yj40
TtLAMQEut6FVGucNZ4z9HDFxRLj9CVvGSd98h1HbHTsRCCuidF1cx5v4PPlB
mHW2n7ZL6SbOx3Q3GK7FkHkFdYCvBotd/QBb3HocHgaCv4szVSOylXLew02w
C1IVXt9TX4Uultiq2//qL3c2RggpMVGMGRP0KN3ZqxnCmOkdIWoqCUvcr3Av
AvDtr8ZzxX2IRvrfgTluTooQYXoVkvh9N9rxat0FI7Ud8UnMiZNwL1dIuTT1
SZDEbIYRQ3x/RAO7BbOkv22QcBmynTco2ZO4yNHWIuij81DnjozvFs0vr+5x
7LsLrLC8k+3HDmsRUu0auAAmFOo=
=DUva
-----END PGP MESSAGE-----
```

The above message was encrypted using the Mailvelope implementation of PGP, as can be seen from the version and comment lines at the beginning of the message. (The version and comment lines may be deleted if you wish, but the "-----BEGIN PGP MESSAGE-----" and "-----END PGP MESSAGE-----" lines must remain for most PGP programs to correctly interpret and decrypt the message.)

Once you received the above message, the PGP software on your computer would decrypt the message and you would be able to read it, assuming that your PGP key ring contained a private key associated with the public key used to encrypt the message. If you had encrypted the above message it would be because you had a copy of the intended recipient's PGP public key. You could then send the encrypted message by e-mail, and only the person with the corresponding PGP private key could decrypt and read the message.

Disadvantages of Using PGP

One possible disadvantage of using PGP encryption with your e-mail is that you must have PGP installed on the computer you are using (or available in a portable PGP version), and you must have your PGP key ring available as well. If you regularly access your e-mail from public computers (i.e. libraries, Internet cafés), or if you access your e-mail from computers that you

don't control (work computers) you probably won't be able to have PGP installed. You may of course install PGP and your PGP key ring on all of your own computers (home computer, laptop, tablet, etc.), and if allowed use Portable PGP on computers that you do not control.

While all PGP implementations support message encryption and decryption, not all implementations of PGP support all PGP functions. For example, at the time this paper was written Mailvelope did not support digitally signing messages. If a particular PGP function is important to you be sure that you choose a PGP implementation that supports that function.

PGP protects the content of your e-mail. It does not however conceal with whom you are exchanging e-mail, nor does it hide the metadata in the messages you send and receive.

For PGP to work, everyone with whom you wish to communicate securely must have PGP installed and you must have exchanged public keys with them. Most current implementations of PGP are very simple to install and use, but individuals with weak computer skills may initially have some trouble understanding how to encrypt and decrypt messages, or use other functions in the PGP program. Even individuals who have no difficulty understanding PGP may not always use it because of the extra couple of mouse clicks or key strokes required to encrypt or decrypt a message. Only people convinced of the importance and value of encryption will regularly use PGP to protect their e-mail communications.

Conclusions

Recently there had been concern that the National Security Agency (NSA) was reading everyone's private e-mail. Before the concerns about the NSA there were concerns that private corporations and e-mail service providers were scanning private e-mails to send targeted advertisements. The threat from hackers, cyber-stalkers, and identity thieves is always a concern, and one that continues to grow as companies report data breaches affecting hundreds-of-millions of people.

PGP will not solve all of your on-line communications security problems, but strong encryption is always a valuable tool for protecting private and sensitive information. By obtaining a copy of PGP and using it to encrypt e-mail that you exchange with friends and family you protect your personal privacy and that of those with whom you communicate. A business or organization that provides a PGP option to its customers and clients demonstrates a commitment to protecting those customers' and clients' privacy rights and safeguarding their personal information.

If you are going to use e-mail, then you should also use PGP.