Gpg4win
Email Security using GnuPG for Windows

By Russ McRee

Prerequisites

Nothing other than a recent Windows OS and the desire to CYA

Similar Projects

Enigmail[1]
PGP (Commercial)[2]

I tire of hearing it, and I'm sure you might as well. Sales people tout it in the products we must buy to secure our environments. Consultants remind us to weave it into our practices. Training programs fill their content with repetitive references to it. What is it, you ask? CIA: confidentiality, integrity, and availability. No need to spend another moment on it; we are all security professionals, and whether or not we tire of hearing it, we are reminded of its importance with an indelible reference seared into our psyche, as a cattle brand might forever tag its bovine target. We know CIA. What's the point? Integral to the confidentiality piece is email encryption. Yes, there are strong commercial products with excellent offerings intended to aid you in this endeavor, but here we focus on a freely available tool that may allow you to achieve the same goals as you would via more costly avenues.

To that end, Gpg4win[3] (GNU Privacy Guard for Windows) is an email encryption suite, the result of a project initiated by the Federal Office for Information Security (BSI), the central IT security service provider for the German government.

GnuPG is the GNU project's complete and free implementation of the OpenPGP standard as defined by RFC4880. GnuPG allows you to encrypt and sign your data and communication, and features a versatile key management system as well as access modules for all kind of public key directories. GnuPG, also known as GPG, is a command line tool with features for easy integration with other applications. A wealth of frontend applications and libraries are available. Version 2 of GnuPG also provides support for S/MIME.

GnuPG is Free Software (meaning that it respects your freedom). It can be freely used, modified and distributed under the terms of the GNU General Public License." [4]

PGP (Pretty Good Privacy) has not been free for many years, but it used to be available on a temporary basis under similar conditions as GnuPG.

Read Stephen Levy's *Crypto: How the Code Rebels Beat the Government Saving Privacy in the Digital Age* for an excellent read and all the PGP history you can absorb.

You can choose all or some of the following modules during installation:

GnuPG	The core; the actual encryption tool
Win	PTA key manager and encryption assistant
GPA	Another key manager
GPGol	A plug-in for Microsoft Outlook 2003 (email encryption)
GPGee	A plug-in for Windows Explorer (file encryption)
Claws Mail	A complete email program including the plug-in for GnuPG

Any reasonably informed security practitioner who has read the appropriate curriculum will remember our friends Bob and Alice and their desire for privacy. No need to play that scratchy record either, but my favorite reads on keypair methodology, aside from the original masterpiece, *"A Method for Obtaining Digital Signatures and Public-Key Cryptosystems"*[5] from Rivest, Shamir, and Adleman, are Erin Spiceland's *"A Simple Guide to Encryption"*[6] (the asymmetric chapter is most relevant here) as well as ye olde Wikipedia entry for GnuPG.[7]

I will apologize in advance to those who are comfortable with the asymmetric key process as it pertains to email and file encryption. Our goal in describing Gpg4win is to also provide an introductory primer for those who may not be as familiar with the process.

1 http://enigmail.mozdev.org
2 http://www.pgp.com
3 http://www.gpg4win.org/index.html
4 http://www.gnupg.org
5 http://people.csail.mit.edu/rivest/Rsapaper.pdf
6 http://fuzzymonkey.net/articles/asymmetrickey.shtml
7 http://en.wikipedia.org/wiki/GNU_Privacy_Guard

Installation

Installation is straightforward and is a simple click-through process, with one exception. If you already have a GnuPG-based application installed on your system, read Appendix B of the *Gpg4win for Novices* manual to learn how to migrate existing keys.

One note for command line users: installation of Gpg4win will result in GnuPG availability at a prompt. Type `gpg –help` for command syntax. Everything we will discuss via the use of a GUI can be performed at the command line.

The Claws-Mail email client is also included and incorporates all the Gpg4win functionality.

Usage

We will assume the use of Outlook 2007 for this article, as GPGol is part of the Gpg4win suite, but Thunderbird users can accomplish all of the concepts discussed here via use of the Enigmail extension. In fact, to validate the described methodology, I traded public keys and encrypted email via my website email account on a Linux box with Thunderbird/Enigmail and my work email on Vista with Outlook 2007/Gpg4win.

First and foremost, you will need to generate a private key. Although you have options, the GNU Privacy Assistant (GPA) is my preferred keyring manager. Open GPA via the Start menu, the first time you do so you will be prompted to generate the key.

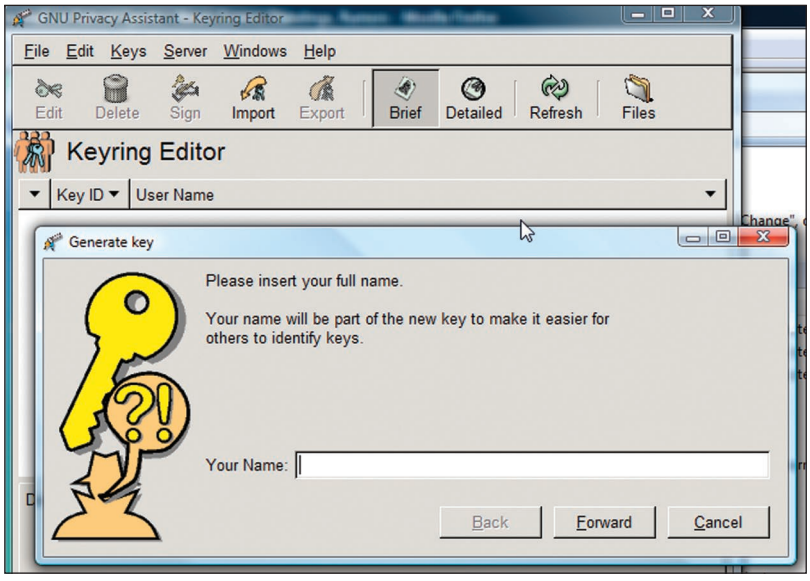

Figure 1 – Generate a private key

Enter your full name, your email address, and a passphrase. My favorite moment during the research for this month's column came when I entered a passphrase that did not meet muster and I was scolded with "Warning: You have entered a passphrase that is obviously not secure." Well, pardon me. But, as we all should, I followed the recommendation, entered some next-level passphrase juju, and moved to the final all-important step of backing up the private key. This is why a strong passphrase is critical as no one should gain access to your private key. Protect it physically and with a strong passphrase.

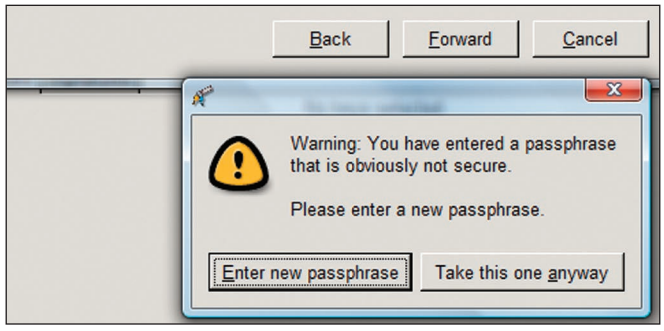

Figure 2 – A passphrase unbecoming

Figure 3 – MIT key server

Newly generated keys in hand, you can begin the process of a public key exchange with those you wish to trade encrypted email or files. You could email your public key as a file for import, sign an email with it, or utilize a public key server. As an example, if you use http://pgp.mit.edu/, submit the key you just created, then your encryption partners can later search and retrieve it.

There is a whole other discussion to be had around key signing, up to and including having key signing parties (Woohoo! Who's bringing the chips?). For a deeper dive into GPG/PGP use, key signing in particular, read *"pgp Key Signing Observations: Overlooked Social and Technical Considerations"* at Linux Security.com and Len Sassaman's *"Efficient Group Key Signing Method."*[8]

One should generally consider signing a key only after the following three requirements have been met in a way that the signer considers acceptable: (1) The fingerprint of the key being signed has been accurately verified, (2) the owner of the key being signed has asserted (or preferably proven) that he *owns* or controls the private component of that key, and (3) the owner has proven that she is who she claims to be, and her key represents her as such.[9]

In Outlook you will find an icon for *WinPT* on the toolbar next to the search window.

8 http://sion.quickie.net/keysigning.txt

9 http://www.linuxsecurity.com/content/view/121645/49

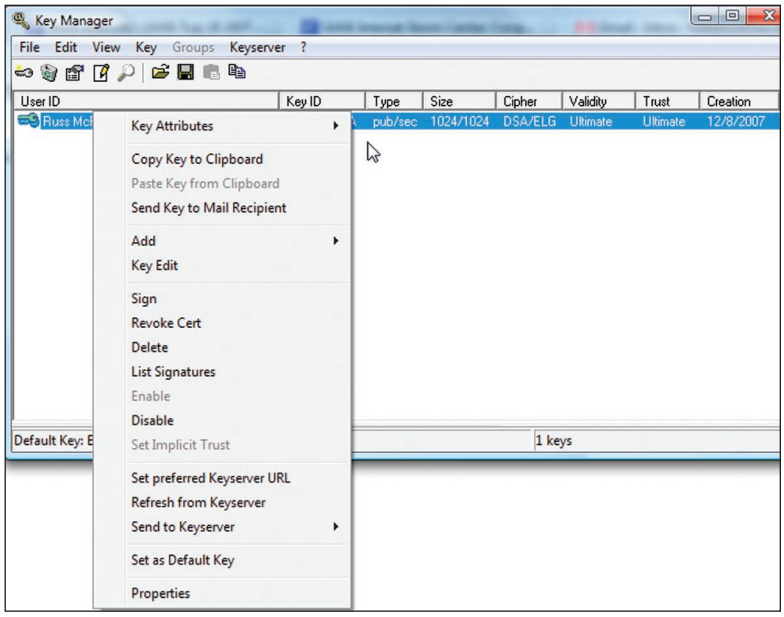

Figure 4 – WinPT Key Manager

Further, as you compose a new message, look for *Add-Ins* on the toolbar and make use of the *Sign* and *Encrypt* icons.

Once you and those you have chosen to exchange with have done so, you can begin to transmit encrypted email and files.

GPGee will assist in the process of encrypting files both asymmetrically and symmetrically. Right-click on the file you wish to protect, select GPGee, then choose PK or Symmetric for encryption, or sign the file.

The result will be an additional file in the directory with a `.gpg` extension. Send this one to the party whose public key you used and delete or protect the original.

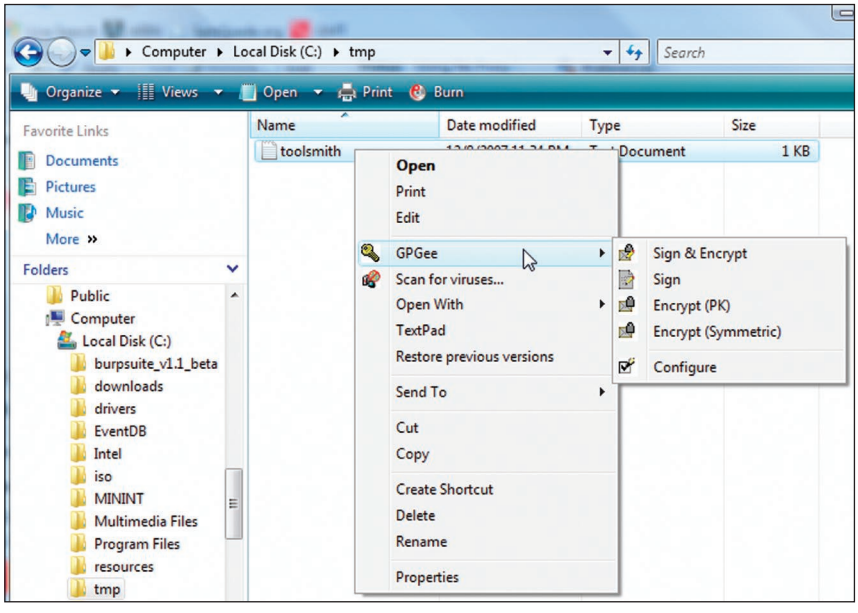

Figure 5 – GPGee

Obviously, if you choose Symmetric, anyone wishing to decrypt must be in possession of the secret key, where the PK option treats files in precisely the same fashion discussed regarding email. So long as your exchange partner has traded public keys with you, you will use their key to encrypt the file and send it along.

Benefits and drawbacks

There may be what some users believe are drawbacks to Gpg4win use, as there are with most email encryption offerings, given the difficulty of getting certain users to adhere to best practices around using it, or overcome the perceived technical difficulty. Often, those who fight email encryption the most are non-technical corporate officers who may be those who would also benefit from it the most. Clear documentation, support, and policy should help alleviate what might otherwise be fatal setbacks in promoting an email encryption program.

Hopefully, the benefits of an added layer of protection to critical or high impact information will outweigh any drawbacks. Gpg4win provides further benefit in its ease of use and simple installation. Paired with Thunderbird/Enigmail for non-Windows or non-Outlook users, the Gpg4win suite can bring great gains to your overall information assurance program.

In conclusion

While the Gpg4win suite, and those like it, provide a reasonable level of protection, nothing is perfect. Ask RSnake how he feels about PGP MITM attacks.[10]

But, simply enough, transmission of private information in the clear can result in data leakage as well as damage to reputation, integrity, and public confidence. Consider giving Gpg4win a spin, particularly in smaller shops with limited budgets and high value information.

Happy New Year and happy signing. Cheers…until next month.

Acknowledgments

Jan-Oliver Wagner, for feedback and insight on Gpg4win

About the Author

Russ McRee, GCIH, GCFA, CISSP, is a security analyst working in the Seattle area. As an advocate of a holistic approach to information security, Russ' website is holisticinfosec.org. Contact him at russ@holisticinfosec.org.

10 http://ha.ckers.org/pgp.html