

What is PGP and GPG?

Scott Fradkin

scott@fradkin.com
<http://tech.fradkin.com>



What is PGP and GPG?

- What this presentation is not
 - Not about the details and implementation
 - Not a discussion of key generation or ciphers
- What it is
 - History
 - How to use
 - What to do with it

What is PGP and GPG?

- What is PGP and GPG?
 - Pretty Good Privacy
 - GNU Privacy Guard
 - Digital signatures and encryption through public key cryptography

What is PGP and GPG?

- Short history of PGP
 - Philip Zimmerman created it in 1991
 - Secure use of BBS systems
 - Securely store messages and files
 - Zimmerman investigated by US Govt. in 1993
 - Source code released in book form in 1995
 - PGP Corp. maintains PGP implementation

What is PGP and GPG?

- Short history of GPG
 - OpenPGP RFC (2440) created in July of 1998
 - Werner Koch released version 1 in Sept. 1999
 - Interoperable with PGP
 - November 2006, version 2
 - Open source, no patented or restricted algorithms

What is PGP and GPG?

- What you can do with it
 - Sign email to help the recipient verify your identity
 - Verify the sender's identity for received emails
 - Encrypt email to another PGP/GPG user
 - Encrypt files

What is PGP and GPG?

- Simple to use
 - Generate a key
 - Encrypt a file
 - Import other peoples keys
 - Sign keys
 - Sign and/or encrypt your email

What is PGP and GPG?

- Generating a key
 - `gpg --gen-key`
 - public key encryption
 - generates a private key/public key pair
 - public key should be accessible publicly
 - Don't lose your passphrase

What is PGP and GPG?

- Revocation certificate
 - `gpg --output revoke.asc --gen-revoke <keyid>`

What is PGP and GPG?

- Encrypting any data file
 - `gpg --output doc.gpg --encrypt --recipient <keyid> doc`
 - `gpg --output doc --decrypt doc.gpg`
 - The recipient must use their private key's passphrase to decrypt

What is PGP and GPG?

- Listing keys in your keyring
 - `gpg --list-keys`

What is PGP and GPG?

- Exporting your key
 - `gpg --output key.gpg --export <keyid>`
 - `gpg --armor --export <keyid>`
 - `gpg --keyserver pgp.mit.edu --send-key <keyid>`

What is PGP and GPG?

- Importing and signing a key
 - `gpg --import akey.gpg`
 - `gpg --keyserver pgp.mit.edu --recv-keys <keyid>`
 - `gpg --fingerprint <keyid>`
 - `gpg --sign-key <keyid>`
 - `gpg --default-key <your default keyid> --sign-key <keyid>`
 - `gpg --keyserver pgp.mit.edu --send-key <keyid>`

What is PGP and GPG?

- Web of Trust
 - Can set trust levels on each key you have in your keyring
 - View the other signers that have signed keys in your keyring
 - How well do you trust the key owners or the other signers?

What is PGP and GPG?

- User Interfaces
 - There are a number of different user interfaces for PGP and GPG for the various operating systems.
 - From the various command lines above, you can see how it's nice to have a UI
 - I use Enigmail for Thunderbird
 - It not only provides email signing and encryption, but full key management of your keyring

What is PGP and GPG?

- Signing email
 - Enigmail for Thunderbird

What is PGP and GPG?

- Encrypting email
 - Enigmail for Thunderbird

What is PGP and GPG?

- Proving your identity
 - Eventually, enough people will have signed your key to validate your identity
 - Could be a spam solution
 - Secret messages and files are cool

What is PGP and GPG?

- **Information**

- http://en.wikipedia.org/wiki/Pretty_Good_Privacy
- http://en.wikipedia.org/wiki/GNU_Privacy_Guard
- <http://www.openpgp.org/>
- <http://www.pgp.com/>
- <http://www.gnupg.org/>
- <http://www.ietf.org/rfc/rfc2440.txt>
- <http://www.gnupg.org/gph/en/manual.html>
- http://cryptnet.net/fdp/crypto/keysigning_party/en/keysigning_party.ht
- [http://www.gnupg.org/\(en\)/related_software/frontends.html](http://www.gnupg.org/(en)/related_software/frontends.html)