How to use GPG

Alternately: PGP SUCKS

Eric C.“echarlie” Landgraf

VTLUUG

November 20, 2017

Contents

History of PGP

- some history here

Versions of PGP

PGP Sucks

- PGP Sucks
  - A lot

PGP needs to die

- better alternatives exist
- reop (tedunangst)
- plain old s/mime with ca-cert

Pragmatic PGP

Still want to use PGP?

- you're insane, but fine

Trust models

- most useful feature of PGP is it's sense of "trust"
- Download a key off a keyserver and look at it; PGP will say whether it is trusted or not; this is configurable

Threat models

- PGP does not defend you against all known attacks! The crypto is secure, but only if you know what it does!
- Your data and PGP key are encrypted at rest, which is great unless someone installs a keylogger.
- Pew has copies of my (encrypted) PGP subkeys—should I revoke

Actually using it

You'll need an implementation of the openPGP tools:

- GNU Privacy Guard (gnupg or GPG) is most common; *nix and windows distributions are available
- I have no experience with GPG4Win, or any non-GPG tools

Demo

Here’s where I switch over to a terminal and generate a key, then do some things with it

Email tools

- mutt has built-in support
- thunderbird through enigmail
- mail.app on osx through some plugin

password management

- pass

Enumerate example

1. Enumerated items are coloured just like itemize
   1.1 and have the same heirarchy, too!
      1.1.1 Just to make it obvious..
   1.2 they come from the “gold” part of the web palette
2. Also notice that the navigation icons are in the blue of the web palette