NeoPG

A replacement for GnuPG

Marcus Brinkmann · 34c3 · Leipzig (2017)

GnuPG

490,000 lines of C code over 20 years

- ~400 command line options
- ~~one~~ two OpenPGP parser
- HTTP client, DNS resolver
- Next: TLS library

OpenPGP

RFC2440 (1998), RFC4880 (2007)

- Harmful: Allows MD5, IDEA, photo ids, etc.
- Mandatory: DSA, ElGamal, 3DES
- Not supported: EdDSA, AEAD
- SHA-1 fingerprints
- Signatures use short key ID (64 bit)

> *"[...] there is not sufficient interest to successfully complete the work of the [OpenPGP] working group."*
> *– IESG Secretary, 11 Nov 2017*

NeoPG

Opionated fork of GnuPG 2

- **1st** refactor and strip down legacy code
- **2nd** replace it with a library and new CLI
- **3rd** implement new features

Status: 250,000 LoC legacy + 2,100 LoC new

-240,000 LoC, -120 command line options

in 3 months!

New command line interface

- Git-style subcommands
  ```
  neopg armor --help
  ```
- Compatibility interface
  ```
  neopg gpg2 ...
  ```
- Color output!
- Better error messages

Packaging

- One repository
- Easy to build with cmake
- Platforms: Linux/BSD, MacOS
- Planned: Windows, Android, iOS

`libneopg`

- easy high level interface
- full low level interface
- control over policy:
  - *key management*
  - *trust models*
  - *data processing (passwords)*

Delegate

- C++11 (GCC, Clang, MSVC)
- STL and Boost
- Curl, SQLite
- Botan (crypto)

Focus on Code Quality

- Continuous Integration
- Static code analysis
- Fuzzing
- Linting, Source Code Formatting (clang-format)

Beyond the web of trust

- Decentralised (Autocrypt, PEP)
- Centralised (keybase.io, Mailvelope Key Server)
- Other (Google End-to-End)

Example keybase.io:

```
$ neopg tweet @lambdafu "Any plans?"
```

Beyond OpenPGP

- Write minimal OpenPGP profile
- Extend OpenPGP (e.g. PQ crypto)
- Use OpenPGP trust anchors for other protocols (e.g. Signal)

🌐 neopg.io

🐦 @neopg_