WIKIPEDIA

GNU Privacy Guard

GNU Privacy Guard (**GnuPG** or **GPG**) is a free-software replacement for Symantec's PGP cryptographic software suite. It is compliant with RFC 4880, the IETF standards-track specification of OpenPGP. Modern versions of PGP are interoperable with GnuPG and other OpenPGP-compliant systems.[4]

GnuPG is part of the GNU Project and received major funding from the German government in 1999.[5]

Contents

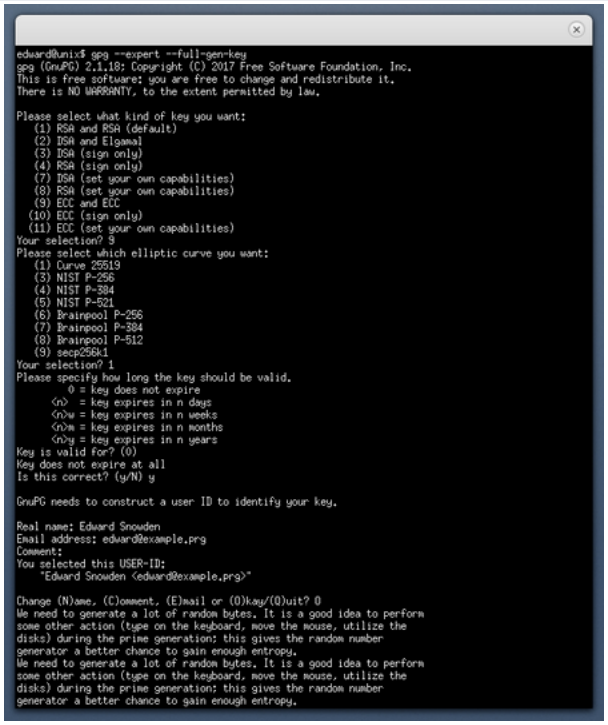
Overview

GnuPG is a hybrid-encryption software program because it uses a combination of conventional symmetric-key cryptography for speed, and public-key cryptography for ease of secure key exchange, typically by using the recipient's public key to encrypt a session key which is used only once. This mode of operation is part of the OpenPGP standard and has been part of PGP from its first version.

The GnuPG 1.x series uses an integrated cryptographic library, while the GnuPG 2.x series replaces this with Libgcrypt.

GNU Privacy Guard

GnuPG



```
edward@unix$ gpg --expert --full-gen-key
gpg (GnuPG) 2.1.18; Copyright (C) 2017 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Please select what kind of key you want:
   (1) RSA and RSA (default)
   (2) DSA and Elgamal
   (3) DSA (sign only)
   (4) RSA (sign only)
   (7) DSA (set your own capabilities)
   (8) RSA (set your own capabilities)
   (9) ECC and ECC
  (10) ECC (sign only)
  (11) ECC (set your own capabilities)
Your selection? 9
Please select which elliptic curve you want:
   (1) Curve 25519
   (3) NIST P-256
   (4) NIST P-384
   (5) NIST P-521
   (6) Brainpool P-256
   (7) Brainpool P-384
   (8) Brainpool P-512
   (9) secp256k1
Your selection? 1
Please specify how long the key should be valid.
         0 = key does not expire
      <n>  = key expires in n days
      <n>w = key expires in n weeks
      <n>m = key expires in n months
      <n>y = key expires in n years
Key is valid for? (0)
Key does not expire at all
Is this correct? (y/N) y

GnuPG needs to construct a user ID to identify your key.

Real name: Edward Snowden
Email address: edward@example.prg
Comment:
You selected this USER-ID:
    "Edward Snowden <edward@example.prg>"

Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? O
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
```

Key pair generation process in Unix terminal emulator

Original author(s)	Werner Koch
Developer(s)	GNU Project
Initial release	7 September 1999[1]
Stable release(s) [±] (https://en.wikipedia.org/wiki/Template:Latest_stable_software_release/GNU_Privacy_Guard?action=edit)	
Modern	2.2.27 / January 11, 2021[2]
Classic	1.4.23 / June 11, 2018[3]
Preview release(s) [±] (https://en.wikipedia.org/wiki/Template:Latest_preview_software_release/GNU_Privacy_Guard?action=edit)	

Repository	dev.gnupg.org /source/gnupg/ (https://dev.gnupg.org/source/gnupg/)
Written in	C
Operating system	Microsoft Windows, macOS, RISC OS, Android, Linux
Type	OpenPGP
License	GPLv3
Website	gnupg.org (https://gnupg.org/)

GnuPG encrypts messages using asymmetric key pairs individually generated by GnuPG users. The resulting public keys may be exchanged with other users in a variety of ways, such as Internet key servers. They must always be exchanged carefully to prevent identity spoofing by corrupting public key ⇔ "owner" identity correspondences. It is also possible to add a cryptographic digital signature to a message, so the message integrity and sender can be verified, if a particular correspondence relied upon has not been corrupted.

GnuPG also supports symmetric encryption algorithms. By default, GnuPG uses the AES symmetrical algorithm since version 2.1,[6] CAST5 was used in earlier versions. GnuPG does not use patented or otherwise restricted software or algorithms. Instead, GnuPG uses a variety of other, non-patented algorithms.[7]

For a long time it did not support the IDEA encryption algorithm used in PGP. It was in fact possible to use IDEA in GnuPG by downloading a plugin for it, however this might require a license for some uses in countries in which IDEA was patented. Starting with versions 1.4.13 and 2.0.20, GnuPG supports IDEA because the last patent of IDEA expired in 2012. Support of IDEA is intended "to get rid of all the questions from folks either trying to decrypt old data or migrating keys from PGP to GnuPG",[8] and hence is not recommended for regular use.

As of 2.2 versions GnuPG supports the following algorithms:

Public key
RSA, ElGamal, DSA, ECDH, ECDSA, EdDSA
Cipher
3DES, IDEA (since versions 1.4.13 and 2.0.20), CAST5, Blowfish, Twofish, AES-128, AES-192, AES-256, Camellia-128, -192 and -256 (since versions 1.4.10 and 2.0.12)
Hash
MD5, SHA-1, RIPEMD-160, SHA-256, SHA-384, SHA-512, SHA-224
Compression
Uncompressed, ZIP, ZLIB, BZIP2

More recent releases of GnuPG 2.x ("modern" and the now deprecated "stable" series) expose most cryptographic functions and algorithms Libgcrypt (its cryptography library) provides, including support for elliptic curve cryptography (ECDH, ECDSA and EdDSA)[9] in the "modern" series (i.e. since GnuPG 2.1).

History

GnuPG was initially developed by Werner Koch.[10][11] The first production version, version 1.0.0, was released on September 7, 1999, almost two years after the first GnuPG release (version 0.0.0).[1][10] The German Federal Ministry of Economics and Technology funded the documentation and the port to Microsoft Windows in 2000.[11]

GnuPG is a system compliant to the OpenPGP standard, thus the history of OpenPGP is of importance; it was designed to interoperate with PGP, an email encryption program initially designed and developed by Phil

Zimmermann.[12][13]

On February 7, 2014, a GnuPG crowdfunding effort closed, raising €36,732 for a new Web site and infrastructure improvements.[14]

Branches

As of January 2018, there are two actively maintained branches of GnuPG:

- "Modern" (2.2), with numerous new features, such as elliptic curve cryptography, compared to the former "stable" (2.0) branch, which it replaced with the release of GnuPG 2.2.0 on August 28, 2017.[15] It was initially released on November 6, 2014.[9]
- "Classic" (1.4), the older, but still maintained standalone version, most suitable for older or embedded platforms. Initially released on December 16, 2004.[16]

Different GnuPG 2.x versions (e.g. from the 2.2 and 2.0 branches) cannot be installed at the same time. However, it is possible to install a "classic" GnuPG version (i.e. from the 1.4 branch) along with any GnuPG 2.x version.[9]

Before the release of GnuPG 2.2 ("modern"), the now deprecated "stable" branch (2.0) was recommended for general use, initially released on November 13, 2006.[17] This branch reached its end-of-life on December 31, 2017;[18] Its last version is 2.0.31, released on December 29, 2017.[19]

Before the release of GnuPG 2.0, all stable releases originated from a single branch; i.e., before November 13, 2006, no multiple release branches were maintained in parallel. These former, sequentially succeeding (up to 1.4) release branches were:

- 1.2 branch, initially released on September 22, 2002,[20] with 1.2.6 as the last version, released on October 26, 2004.[21]
- 1.0 branch, initially released on September 7, 1999,[1] with 1.0.7 as the last version, released on April 30, 2002.[22]

(Note that branches with an odd minor release number (e.g. 2.1, 1.9, 1.3) are development branches leading to a stable release branch with a "+ 0.1" higher version number (e.g. 2.2, 2.0, 1.4), hence branches 2.2 and 2.1 both belong to the "modern" series, 2.0 and 1.9 both to the "stable" series, while the branches 1.4 and 1.3 both belong to the "classic" series.)

Platforms

Although the basic GnuPG program has a command-line interface, there exists various front-ends that provide it with a graphical user interface. For example, GnuPG encryption support has been integrated into KMail and Evolution, the graphical email clients found in KDE and GNOME, the most popular Linux desktops. There are also graphical GnuPG front-ends, for example Seahorse for GNOME and KGPG for KDE.

The GPG Suite project provides a number of Aqua front-ends for OS integration of encryption and key management as well as GnuPG installations via Installer packages[23] for macOS. Furthermore, the GPG Suite Installer[24] installs all related OpenPGP applications (GPG Keychain Access), plugins (GPGMail) and dependencies (MacGPG) to use GnuPG based encryption.

Instant messaging applications such as Psi and Fire can automatically secure messages when GnuPG is installed and configured. Web-based software such as Horde also makes use of it. The cross-platform extension Enigmail provides GnuPG support for Mozilla Thunderbird and SeaMonkey. Similarly, Enigform provides GnuPG support for Mozilla Firefox. FireGPG was discontinued June 7, 2010.[25]

In 2005, g10 Code GmbH and Intevation GmbH released Gpg4win, a software suite that includes GnuPG for Windows, GNU Privacy Assistant, and GnuPG plug-ins for Windows Explorer and Outlook. These tools are wrapped in a standard Windows installer, making it easier for GnuPG to be installed and used on Windows systems.

Limitations

As a command-line-based system, GnuPG 1.x is not written as an API that may be incorporated into other software. To overcome this, *GPGME* (abbreviated from *GnuPG Made Easy*) was created as an API wrapper around GnuPG that parses the output of GnuPG and provides a stable and maintainable API between the components.[26] This currently requires an out-of-process call to the GnuPG executable for many GPGME API calls; as a result, possible security problems in an application do not propagate to the actual crypto code due to the process barrier. Various graphical front-ends based on GPGME have been created.

Since GnuPG 2.0, many of GnuPG's functions are available directly as C APIs in Libgcrypt.[27]

Vulnerabilities

The OpenPGP standard specifies several methods of digitally signing messages. In 2003, due to an error in a change to GnuPG intended to make one of those methods more efficient, a security vulnerability was introduced.[28] It affected only one method of digitally signing messages, only for some releases of GnuPG (1.0.2 through 1.2.3), and there were fewer than 1000 such keys listed on the key servers.[29] Most people did not use this method, and were in any case discouraged from doing so, so the damage caused (if any, since none has been publicly reported) would appear to have been minimal. Support for this method has been removed from GnuPG versions released after this discovery (1.2.4 and later).

Two further vulnerabilities were discovered in early 2006; the first being that scripted uses of GnuPG for signature verification may result in false positives,[30] the second that non-MIME messages were vulnerable to the injection of data which while not covered by the digital signature, would be reported as being part of the signed message.[31] In both cases updated versions of GnuPG were made available at the time of the announcement.

In June 2017, a vulnerability (CVE-2017-7526) was discovered within Libgcrypt by Bernstein, Breitner and others: a library used by GnuPG, which enabled a full key recovery for RSA-1024 and about more than 1/8th of RSA-2048 keys. This side-channel attack exploits the fact that Libgcrypt used a sliding windows method for exponentiation which leads to the leakage of exponent bits and to full key recovery.[32][33] Again, an updated version of GnuPG was made available at the time of the announcement.

In October 2017, the ROCA vulnerability was announced that affects RSA keys generated by YubiKey 4 tokens, which often are used with PGP/GPG. Many published PGP keys were found to be susceptible.[34]

Around June 2018, the SigSpoof attacks were announced. These allowed an attacker to convincingly spoof digital signatures.[35][36]

Application support

Notable applications, front ends and browser extensions that support GPG include the following:

- Claws Mail – an email client with GPG plugin
- Enigmail – a Mozilla Thunderbird and SeaMonkey extension
- Evolution – a GNOME Mail application with native GnuPG support
- FireGPG – a Firefox extension (discontinued)
- Gnus – a message and news reader in GNU Emacs
- Gpg4win – a Windows package with tools and manuals for email and file encryption
- GPGMail – a macOS Mail.app plug-in
- KGPG – a KDE graphical front end for GnuPG
- KMail – email client / email component of Kontact (PIM software), that uses GPG for cryptography
- MCabber – a Jabber client
- Mailvelope – a Google Chrome and Firefox extension for end-to-end encryption of email traffic
- Mutt – an email client with PGP/GPG support built-in
- Psi (instant messaging client)
- The Bat! – email client, that can use GnuPG as an OpenPGP provider
- WinPT – a graphical front end to GPG for Windows (discontinued)

In popular culture

In May 2014, *The Washington Post* reported on a 12-minute video guide "GPG for Journalists" posted to Vimeo in January 2013[37] by a user named anon108. The *Post* identified anon108 as fugitive NSA whistleblower Edward Snowden, who it said made the tutorial—"narrated by a digitally disguised voice whose speech patterns sound similar to those of Snowden"—to teach journalist Glenn Greenwald email encryption. Greenwald said that he could not confirm the authorship of the video.[38] There is a similarity between the tutorial and interviews Snowden has participated in, such as mentioning a password of "margaretthatcheris110%sexy" in both this video and an interview conducted with John Oliver in 2015.[39]

See also

- Acoustic cryptanalysis
- Key signing party
- Off-the-Record Messaging – also known as OTR
- OpenPGP card – a smartcard with many GnuPG functions
- Package manager
- RetroShare – a friend-to-friend network based on PGP authentication

- Web of trust

References

1. "Release Notes" (https://gnupg.org/download/release_notes.html). GnuPG. Archived (https://web.archive.org/web/20140209040746/http://gnupg.org/download/release_notes.html) from the original on 2014-02-09. Retrieved 2014-01-30.
2. Koch, Werner (2021-01-11). "[Announce] GnuPG 2.2.27 released" (https://lists.gnupg.org/pipermail/gnupg-announce/2021q1/000452.html). *gnupg-announce* (Mailing list). Retrieved 2021-01-11.
3. "NEWS file" (https://files.gnupg.net/file/data/l7t365j2rdge5saveiqd/PHID-FILE-4sgc5wrbpqzioi6bn7lt/NEWS). Noteworthy changes in version 1.4.23 (2018-06-11) heading. Retrieved 13 June 2018.
4. "Gnu Privacy Guard" (https://www.gnupg.org/faq/gnupg-faq.html#compatible). GnuPG.org. Archived (https://web.archive.org/web/20150429192132/https://www.gnupg.org/faq/gnupg-faq.html#compatible) from the original on 2015-04-29. Retrieved 2015-05-26.
5. "Bundesregierung fördert Open Source" (http://www.heise.de/newsticker/meldung/Bundesregierung-foerdert-Open-Source-24110.html) (in German). Heise Online. 1999-11-15. Archived (https://web.archive.org/web/20131012024601/http://www.heise.de/newsticker/meldung/Bundesregierung-foerdert-Open-Source-24110.html) from the original on October 12, 2013. Retrieved July 24, 2013.
6. "[Announce] The maybe final Beta for GnuPG 2.1" (https://lists.gnupg.org/pipermail/gnupg-announce/2014q4/000357.html). Archived (https://web.archive.org/web/20190502211129/https://lists.gnupg.org/pipermail/gnupg-announce/2014q4/000357.html) from the original on 2019-05-02. Retrieved 2019-03-28.
7. "GnuPG Features" (https://www.gnupg.org/features.en.html). Archived (https://web.archive.org/web/20091004174134/http://www.gnupg.org/features.en.html) from the original on October 4, 2009. Retrieved October 1, 2009.
8. Koch, Werner (2012-12-21). "GnuPG 1.4.13 released" (http://lists.gnupg.org/pipermail/gnupg-users/2012-December/045844.html) (Mailing list). gnupg-users. Archived (https://web.archive.org/web/20130212065951/http://lists.gnupg.org/pipermail/gnupg-users/2012-December/045844.html) from the original on 2013-02-12. Retrieved 2013-05-19.
9. Koch, Werner (2014-11-06). "[Announce] GnuPG 2.1.0 "modern" released" (http://lists.gnupg.org/pipermail/gnupg-announce/2014q4/000358.html). gnupg.org. Archived (https://web.archive.org/web/20141106154709/http://lists.gnupg.org/pipermail/gnupg-announce/2014q4/000358.html) from the original on 2014-11-06. Retrieved 2014-11-06.
10. Angwin, Julia (5 February 2015). "The World's Email Encryption Software Relies on One Guy, Who is Going Broke" (https://www.propublica.org/article/the-worlds-email-encryption-software-relies-on-one-guy-who-is-going-broke). ProPublica. Archived (https://web.archive.org/web/20150206005618/http://www.propublica.org/article/the-worlds-email-encryption-software-relies-on-one-guy-who-is-going-broke) from the original on 6 February 2015. Retrieved 6 February 2015.

11. Wayner, Peter (19 November 1999). "Germany Awards Grant for Encryption" (http://partners.nytimes.com/library/tech/99/11/cyber/articles/19encrypt.html). *The New York Times*. Archived (https://web.archive.org/web/20140825204940/http://partners.nytimes.com/library/tech/99/11/cyber/articles/19encrypt.html) from the original on 25 August 2014. Retrieved 2014-08-08.
12. "Gnu Privacy Guard" (https://web.archive.org/web/20140227185009/http://openpgp.org/members/gnupg.shtml). OpenPGP.org. Archived from the original (http://www.openpgp.org/members/gnupg.shtml) on 2014-02-27. Retrieved 2014-02-26.
13. "Where to Get PGP" (https://philzimmermann.com/EN/findpgp/). Philzimmermann.com. Archived (https://web.archive.org/web/20140226011248/http://philzimmermann.com/EN/findpgp/) from the original on 2014-02-26. Retrieved 2014-02-26.
14. "GnuPG: New web site and infrastructure" (http://goteo.org/project/gnupg-new-website-and-infrastructure/home). goteo.org. Archived (https://web.archive.org/web/20140330103240/http://goteo.org/project/gnupg-new-website-and-infrastructure/home) from the original on 2014-03-30. Retrieved 2014-03-09.
15. Koch, Werner (2017-08-28). "[Announce] GnuPG 2.2.0 released" (https://lists.gnupg.org/pipermail/gnupg-announce/2017q3/000413.html). *gnupg-announce* (Mailing list). Archived (https://web.archive.org/web/20170829040530/https://lists.gnupg.org/pipermail/gnupg-announce/2017q3/000413.html) from the original on 2017-08-29. Retrieved 2017-09-21.
16. Koch, Werner (2004-12-16). "[Announce] GnuPG stable 1.4 released" (http://lists.gnupg.org/pipermail/gnupg-announce/2004q4/000186.html). gnupg.org. Archived (https://web.archive.org/web/20050103172907/http://lists.gnupg.org/pipermail/gnupg-announce/2004q4/000186.html) from the original on 2005-01-03. Retrieved 2004-12-16.
17. Koch, Werner (2006-11-13). "[Announce] GnuPG 2.0 released" (http://lists.gnupg.org/pipermail/gnupg-announce/2006q4/000239.html). gnupg.org. Archived (https://web.archive.org/web/20140214124626/http://lists.gnupg.org/pipermail/gnupg-announce/2006q4/000239.html) from the original on 2014-02-14. Retrieved 2014-01-30.
18. Koch, Werner (2017-01-23). "[Announce] GnuPG 2.1.18 released" (https://lists.gnupg.org/pipermail/gnupg-announce/2017q1/000401.html). gnupg.org. Archived (https://web.archive.org/web/20170211080210/https://lists.gnupg.org/pipermail/gnupg-announce/2017q1/000401.html) from the original on 2017-02-11. Retrieved 2017-02-04.
19. "GnuPG 2.0.31" (https://dev.gnupg.org/rGe6dae418c260592c0860519481b5eb92d14329db). 2017-12-29. Retrieved 2017-12-30.
20. Koch, Werner (2002-09-06). "[Announce]GnuPG 1.2 released" (http://lists.gnupg.org/pipermail/gnupg-announce/2002q3/000136.html). gnupg.org. Archived (https://web.archive.org/web/20140617075459/http://lists.gnupg.org/pipermail/gnupg-announce/2002q3/000136.html) from the original on 2014-06-17. Retrieved 2014-11-06.
21. Koch, Werner (2004-08-26). "[Announce] GnuPG 1.2.6 released" (http://lists.gnupg.org/pipermail/gnupg-announce/2004q3/000176.html). gnupg.org. Archived (https://web.archive.org/web/20140617075605/http://lists.gnupg.org/pipermail/gnupg-announce/2004q3/000176.html) from the original on 2014-06-17. Retrieved 2014-11-06.
22. Koch, Werner (2002-04-30). "[Announce] GnuPG 1.0.7 released" (http://lists.gnupg.org/pipermail/gnupg-announce/2002q2/000135.html). gnupg.org. Archived (https://web.archive.org/web/20140617075617/http://lists.gnupg.org/pipermail/gnupg-announce/2002q2/000135.html) from the original on 2014-06-17. Retrieved 2014-11-06.

23. "*Mac GPG Suite*" (https://gpgtools.org/). *GPG Suite. Retrieved 2017-12-24.*
24. "*Mac GPG Suite installer*" (https://gpgtools.org/gpgsuite.html). *GPG Suite. Retrieved 2017-12-24.*
25. "FireGPG's developers blog" (http://blog.getfiregpg.org/2010/06/07/firegpg-discontinued/). Archived (https://web.archive.org/web/20130727112311/http://blog.getfiregpg.org/2010/06/07/firegpg-discontinued/) from the original on July 27, 2013. Retrieved July 24, 2013.
26. "GPGME (GnuPG Made Easy)" (https://www.gnupg.org/%28it%29/related_software/gpgme/index.html). *gnupg.org*. February 11, 2015. Archived (https://web.archive.org/web/20150217100145/https://www.gnupg.org/%28it%29/related_software/gpgme/index.html) from the original on February 17, 2015. Retrieved March 3, 2015.
27. "Libraries" (https://www.gnupg.org/related_software/libraries.en.html#lib-libgcrypt). *GNUPG*. Archived (https://web.archive.org/web/20151208072115/https://www.gnupg.org/related_software/libraries.en.html#lib-libgcrypt) from the original on 8 December 2015. Retrieved 2 December 2015.
28. Nguyen, Phong Q. "Can We Trust Cryptographic Software? Cryptographic Flaws in GNU Privacy Guard v1.2.3" (https://www.di.ens.fr/~pnguyen/pub_Ng04.htm). EUROCRYPT 2004: 555–570. Archived (https://web.archive.org/web/20171204133110/http://www.di.ens.fr/~pnguyen/pub_Ng04.htm) from the original on 2017-12-04. Retrieved 2019-08-23.
29. Koch, Werner (November 27, 2003). "GnuPG's ElGamal signing keys compromised" (http://lists.gnupg.org/pipermail/gnupg-announce/2003q4/000160.html). Archived (https://web.archive.org/web/20040318174334/http://lists.gnupg.org/pipermail/gnupg-announce/2003q4/000160.html) from the original on March 18, 2004. Retrieved May 14, 2004.
30. Koch, Werner (February 15, 2006). "False positive signature verification in GnuPG" (http://lists.gnupg.org/pipermail/gnupg-announce/2006q1/000211.html). Archived (https://web.archive.org/web/20060617192634/http://lists.gnupg.org/pipermail/gnupg-announce/2006q1/000211.html) from the original on June 17, 2006. Retrieved May 23, 2006.
31. Koch, Werner (March 9, 2006). "GnuPG does not detect injection of unsigned data" (http://lists.gnupg.org/pipermail/gnupg-announce/2006q1/000218.html). Archived (https://web.archive.org/web/20060505205727/http://lists.gnupg.org/pipermail/gnupg-announce/2006q1/000218.html) from the original on May 5, 2006. Retrieved May 23, 2006.
32. Edge, Jake (5 July 2017). "Breaking Libgcrypt RSA via a side channel" (https://lwn.net/Articles/727179/). *LWN.net*. Archived (https://web.archive.org/web/20170728155905/https://lwn.net/Articles/727179/) from the original on 28 July 2017. Retrieved 28 July 2017.
33. "Sliding right into disaster: Left-to-right sliding windows leak" (https://eprint.iacr.org/2017/627.pdf) (PDF). Archived (https://web.archive.org/web/20170630170347/https://eprint.iacr.org/2017/627.pdf) (PDF) from the original on 2017-06-30. Retrieved 2017-06-30.
34. The Return of Coppersmith's Attack: Practical Factorization of Widely Used RSA Moduli (https://crocs.fi.muni.cz/_media/public/papers/nemec_roca_ccs17_preprint.pdf) Archived (https://web.archive.org/web/20171112012916/https://crocs.fi.muni.cz/_media/public/papers/nemec_roca_ccs17_preprint.pdf) 2017-11-12 at the Wayback Machine, Matus Nemec, Marek Sys, Petr Svenda, Dusan Klinec,Vashek Matyas, November 2017

35. "Archived copy" (https://arstechnica.com/information-technology/2018/06/decades-old-pgp-bug-allowed-hackers-to-spoof-just-about-anyones-signature/). Archived (https://web.archive.org/web/20180907110403/https://arstechnica.com/information-technology/2018/06/decades-old-pgp-bug-allowed-hackers-to-spoof-just-about-anyones-signature/) from the original on 2018-09-07. Retrieved 2018-09-07.
36. "Archived copy" (https://www.theregister.co.uk/2018/06/19/gnupg_popped_again_in_pass/). Archived (https://web.archive.org/web/20180630114100/https://www.theregister.co.uk/2018/06/19/gnupg_popped_again_in_pass/) from the original on 2018-06-30. Retrieved 2018-09-07.
37. "GPG for Journalists - Windows edition - Encryption for Journalists" (https://vimeo.com/56881481). *Vimeo*. Archived (https://web.archive.org/web/20161024180320/https://vimeo.com/56881481) from the original on 2016-10-24. Retrieved 2016-10-14.
38. Peterson, Andrea (May 14, 2014). "Edward Snowden sent Glenn Greenwald this video guide about encryption for journalists. Greenwald ignored it" (https://www.washingtonpost.com/blogs/the-switch/wp/2014/05/14/edward-snowden-sent-glenn-greenwald-this-video-guide-about-encryption-for-journalists-greenwald-ignored-it/). *The Washington Post*. Archived (https://web.archive.org/web/20150623084152/http://www.washingtonpost.com/blogs/the-switch/wp/2014/05/14/edward-snowden-sent-glenn-greenwald-this-video-guide-about-encryption-for-journalists-greenwald-ignored-it/) from the original on June 23, 2015. Retrieved August 28, 2017.
39. "Edward Snowden on Passwords: Last Week Tonight with John Oliver (HBO)" (https://www.youtube.com/watch?v=yzGzB-yYKcc). *YouTube*. Archived (https://web.archive.org/web/20200717142358/https://www.youtube.com/watch?v=yzGzB-yYKcc) from the original on 17 July 2020. Retrieved 17 July 2020.

External links

- Official website (https://gnupg.org/)
- A Short History of the GNU Privacy Guard (https://lists.gnupg.org/pipermail/gnupg-announce/2007q4/000268.html), written by Werner Koch, published on GnuPG's 10th birthday

Retrieved from "https://en.wikipedia.org/w/index.php?title=GNU_Privacy_Guard&oldid=1000389336"

This page was last edited on 14 January 2021, at 22:10 (UTC).