GnuPG: Past, Present, and Future

Werner Koch

DebConf15 — Heidelberg
August 16, 2015
Outline

Past

Present

Future
PGP-2 and the year was 1991

- First public available crypto tool by Phil Zimmermann.
- Heavily improved by Branko Lankester, Colin Plumb, Derek Atkins, Hal Finney, Peter Gutmann, et al.
- Problem 1: RSA patent
- Problem 2: IDEA patent
- Problem 3: Export restrictions
Past Present Future

PGP-2 and the year was 1991

- First public available crypto tool by Phil Zimmermann.
- Heavily improved by Branko Lankester, Colin Plumb, Derek Atkins, Hal Finney, Peter Gutmann, et al.

- Problem 1: RSA patent
- Problem 2: IDEA patent
- Problem 3: Export restrictions
PGP-2 and the year was 1991

- First public available crypto tool by Phil Zimmermann.
- Heavily improved by Branko Lankester, Colin Plumb, Derek Atkins, Hal Finney, Peter Gutmann, et al.

- Problem 1: RSA patent
- Problem 2: IDEA patent
- Problem 3: Export restrictions
PGP-2 and the year was 1991

- First public available crypto tool by Phil Zimmermann.
- Heavily improved by Branko Lankester, Colin Plumb, Derek Atkins, Hal Finney, Peter Gutmann, et al.

- Problem 1: RSA patent
- Problem 2: IDEA patent
- Problem 3: Export restrictions
PGP-2 and the year was 1991

- First public available crypto tool by Phil Zimmermann.
- Heavily improved by Branko Lankester, Colin Plumb, Derek Atkins, Hal Finney, Peter Gutmann, et al.
- Problem 1: RSA patent
- Problem 2: IDEA patent
- Problem 3: Export restrictions
PGP-5 and OpenPGP

- 1996: PGP Inc founded
- Spring 1997: DH patent expired, PGP-5 released
- Autumn 1997: OpenPGP WG chartered
- Spring 1998: PGP Inc bought by NAI (ceased support in 2002)
- Autumn 1998: RFC-2440 published
- Autumn 2007: RFC-4880 published
<table>
<thead>
<tr>
<th>Zeit</th>
<th>Security</th>
<th>New Technologies</th>
</tr>
</thead>
<tbody>
<tr>
<td>9:00-9:30</td>
<td>Heiko Schlichting</td>
<td>Keynote</td>
</tr>
<tr>
<td>9:30-10:30</td>
<td>Norbert Pohlmann</td>
<td>Firewall-Technologien</td>
</tr>
<tr>
<td></td>
<td>Werner Almesberger</td>
<td>ATM und Linux</td>
</tr>
<tr>
<td>10:30-11:30</td>
<td>T. Zieschang</td>
<td>Security und Chipcards</td>
</tr>
<tr>
<td></td>
<td>Dave S. Miller</td>
<td>Linux on Sparc</td>
</tr>
<tr>
<td>11:30-12:30</td>
<td>M. Klische, DCS AG</td>
<td>Biometrische Personenidentifikation</td>
</tr>
<tr>
<td></td>
<td>Stephen R. van den Berg</td>
<td>SPAM, procmail, cucipop</td>
</tr>
<tr>
<td>12:30-13:00</td>
<td>Mittagessen</td>
<td></td>
</tr>
<tr>
<td>13:30-14:30</td>
<td>Andreas Bäß</td>
<td>Status DPN</td>
</tr>
<tr>
<td></td>
<td>Bruce Perens, Pixar Inc.</td>
<td>Debian GNU/Linux</td>
</tr>
<tr>
<td>14:30-15:30</td>
<td>Arttu Huhtiniemi, SolidTech</td>
<td>Database and JAVA</td>
</tr>
<tr>
<td></td>
<td>Stephen R. van den Berg</td>
<td>SPAM, procmail, cucipop</td>
</tr>
<tr>
<td>15:30-16:00</td>
<td>Pause</td>
<td></td>
</tr>
<tr>
<td>16:00-17:00</td>
<td>Gerhard Unger</td>
<td>Secure Computing</td>
</tr>
<tr>
<td></td>
<td>Bettina Kauth, DFN-NOC</td>
<td>Status des B-WIN</td>
</tr>
<tr>
<td>17:00-18:00</td>
<td>Richard Stallman</td>
<td>GNU Current Projects, Ethico-Political issues of free software</td>
</tr>
<tr>
<td>20:00-21:00</td>
<td>Buffet</td>
<td>Geselliger Abend</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Zeit</th>
<th>Security</th>
<th>New Technologies</th>
</tr>
</thead>
<tbody>
<tr>
<td>9:30-10:30</td>
<td>Jörg Ladwein</td>
<td>Security Dynamics</td>
</tr>
<tr>
<td></td>
<td>Jan Vekemans, Vasco</td>
<td>Internet-AcessKey</td>
</tr>
<tr>
<td>10:30-11:30</td>
<td>Lutz Donnerhacke</td>
<td>CA+PGP-Keys</td>
</tr>
<tr>
<td>11:30-13:00</td>
<td>Brunch</td>
<td></td>
</tr>
<tr>
<td>13:00-14:00</td>
<td>Thomas Hetschold, GMD</td>
<td>Secure</td>
</tr>
<tr>
<td></td>
<td>K. Schröter, DOCconnect AG</td>
<td>DOCconnect, Med. Network</td>
</tr>
<tr>
<td>14:00-15:00</td>
<td>Alan Cox</td>
<td>I Pv6</td>
</tr>
<tr>
<td></td>
<td>Progressive Networks</td>
<td>Live Video</td>
</tr>
<tr>
<td>15:00-16:00</td>
<td>D. James Bidzos</td>
<td>Präsident der RSA Inc.</td>
</tr>
</tbody>
</table>
g10 / GnuPG

„Das Briefgeheimnis sowie das Post- und Fernmeldegeheimnis sind unverletzlich. Beschränkungen dürfen nur auf Grund eines Gesetzes angeordnet werden.“

- PGP-5 was non-free
  - even PGP-2 not DFSG compatible
- December 1997: g10 as free PGP-2 replacement
  - No patented algorithms
  - Designed as Unix tool
- Spring 1998: Name now GnuPG, protocol now OpenPGP.
Past Present Future

PAST

g10 / GnuPG

„Das Briefgeheimnis sowie das Post- und Fernmeldegeheimnis sind unverletzlich. Beschränkungen dürfen nur auf Grund eines Gesetzes angeordnet werden.”

- PGP-5 was non-free
  - even PGP-2 not DFSG compatible
- December 1997: g10 as free PGP-2 replacement
  - No patented algorithms
  - Designed as Unix tool
- Spring 1998: Name now GnuPG, protocol now OpenPGP.
g10 / GnuPG

„Das Briefgeheimnis sowie das Post- und Fernmeldegeheimnis sind unverletzlich. Beschränkungen dürfen nur auf Grund eines Gesetzes angeordnet werden.”

- PGP-5 was non-free
  - even PGP-2 not DFSG compatible
- December 1997: g10 as free PGP-2 replacement
  - No patented algorithms
  - Designed as Unix tool
- Spring 1998: Name now GnuPG, protocol now OpenPGP.
Algorithm selection

- **Initial version**
  - Elgamal simply replaced RSA (sign+encrypt)
  - Blowfish as symmetric cipher
  - IDEA as plugin for PGP-2 compatibility in some countries.

- **OpenPGP introduced subkeys**
  - DSA for signatures, Elgamal for encryption.
  - 3DES and CAST5 for symmetric cipher.
  - RSA added in September 2000

- **GnuPG and PGP-{5,6,7}**
  - Worked with Hal Finney and Jon Callas
  - Informal interop testings
  - Testing of new features
Algorithm selection

- **Initial version**
  - Elgamal simply replaced RSA (sign+encrypt)
  - Blowfish as symmetric cipher
  - IDEA as plugin for PGP-2 compatibility in some countries.

- **OpenPGP introduced subkeys**
  - DSA for signatures, Elgamal for encryption.
  - 3DES and CAST5 for symmetric cipher.
  - RSA added in September 2000

- **GnuPG and PGP-{5,6,7}**
  - Worked with Hal Finney and Jon Callas
  - Informal interop testings
  - Testing of new features
GnuPG-2

- g10code founded in 2001
- Bid accepted to implement S/MIME
  - modularized
  - separated crypto library
  - library (gpgme)
GnuPG-2

- g10code founded in 2001
- Bid accepted to implement S/MIME
  - modularized
  - separated crypto library
  - library (gpgme)
Past Present Future

GnuPG-2

- g10code founded in 2001
- Bid accepted to implement S/MIME
  - modularized
  - separated crypto library
  - library (gpgme)
g10 (0.2.7-1) unstable; urgency=low

* Initial release.

-- James Troup <jjtroup@...> Fri, 20 Feb 1998

- gpgv written in 2000 to prepare for signed packages
- 4 years later integrated into apt
- GnuPG-2 packaged in 2004
Past

GnuPG in Debian

g10 (0.2.7-1) unstable; urgency=low

* Initial release.

-- James Troup <jjtroup@...> Fri, 20 Feb 1998

Future

- gpgv written in 2000 to prepare for signed packages
- 4 years later integrated into apt
- GnuPG-2 packaged in 2004
GnuPG in Debian

Past

$\text{g10 (0.2.7-1) unstable; urgency=low}$

$\text{* Initial release.}$

$\text{-- James Troup <jjtroup@...> Fri, 20 Feb 1998}$

Present

$\text{gpgv written in 2000 to prepare for signed packages}$
$\text{4 years later integrated into apt}$
$\text{GnuPG-2 packaged in 2004}$

Future
GnuPG in Debian

Past

Initial release.

-- James Troup <jjtroup@...> Fri, 20 Feb 1998

Present

GPGv written in 2000 to prepare for signed packages
4 years later integrated into apt
GnuPG-2 packaged in 2004

Future
Past

Experimental port to Windows in 1998

Final port to Windows in 2000
  • Thanks to grant from the German government

Gpg4win published in 2006

GnuPG-2 was not designed to be ported
  • . . . but we did it anyway

Surprising number of Gpg4win users

Present

Future
Port to Windows

- Experimental port to Windows in 1998
- Final port to Windows in 2000
  - Thanks to grant from the German government
- Gpg4win published in 2006
- GnuPG-2 was not designed to be ported
  - ...but we did it anyway
- Surprising number of Gpg4win users
Port to Windows

- Experimental port to Windows in 1998
- Final port to Windows in 2000
  - Thanks to grant from the German government
- Gpg4win published in 2006
  - GnuPG-2 was not designed to be ported
    - ...but we did it anyway
- Surprising number of Gpg4win users
Port to Windows

- Experimental port to Windows in 1998
- Final port to Windows in 2000
  - Thanks to grant from the German government
- Gpg4win published in 2006
- GnuPG-2 was not designed to be ported
  - ...but we did it anyway
- Surprising number of Gpg4win users
Port to Windows

- Experimental port to Windows in 1998
- Final port to Windows in 2000
  - Thanks to grant from the German government
- Gpg4win published in 2006
- GnuPG-2 was not designed to be ported
  - ...but we did it anyway
- Surprising number of Gpg4win users
Past Present Future

Outline

Past

Present

Future
Branches

- **Version 2.1 ("modern")**
  - Released November 2014
  - Fixing remaining bugs
  - Adding last features
  - In experimental

- **Version 2.0 ("stable")**
  - Just maintained.
  - Minor changes to help migration to 2.1.

- **Version 1.4 ("classic")**
  - Supported to help with old data and keys.
  - Keeping PGP-2 support.
  - Minor changes to help migration to 2.1.
Branches

- Version 2.1 ("modern")
  - Released November 2014
  - Fixing remaining bugs
  - Adding last features
  - In experimental

- Version 2.0 ("stable")
  - Just maintained.
  - Minor changes to help migration to 2.1.

- Version 1.4 ("classic")
  - Supported to help with old data and keys.
  - Keeping PGP-2 support.
  - Minor changes to help migration to 2.1.
Branches

- Version 2.1 (“modern”)
  - Released November 2014
  - Fixing remaining bugs
  - Adding last features
  - In experimental

- Version 2.0 (“stable”)
  - Just maintained.
  - Minor changes to help migration to 2.1.

- Version 1.4 (“classic”)
  - Supported to help with old data and keys.
  - Keeping PGP-2 support.
  - Minor changes to help migration to 2.1.
OpenPGP WG timeline

Mar 2008  Concluded after RFC-4880

Jun 2015  WG re-chartered

Sep 2015  WG (rough) consensus on updates to RFC-4880.

Feb 2016  First WG I-D for RFC-4880bis

Jul 2016  RFC-4880bis WG I-D final call
OpenPGP WG timeline

Mar 2008  Concluded after RFC-4880
Jun 2015  WG re-chartered
Sep 2015  WG (rough) consensus on updates to RFC-4880.
Feb 2016  First WG I-D for RFC-4880bis
Jul 2016  RFC-4880bis WG I-D final call
OpenPGP WG timeline

Mar 2008  Concluded after RFC-4880
Jun 2015  WG re-chartered
Sep 2015  WG (rough) consensus on updates to RFC-4880.
Feb 2016  First WG I-D for RFC-4880bis
Jul 2016  RFC-4880bis WG I-D final call
OpenPGP WG timeline

Mar 2008  Concluded after RFC-4880
Jun 2015  WG re-chartered
Sep 2015  WG (rough) consensus on updates to RFC-4880.
Feb 2016  First WG I-D for RFC-4880bis
          Jul 2016  RFC-4880bis WG I-D final call
OpenPGP WG timeline

Mar 2008  Concluded after RFC-4880
Jun 2015  WG re-chartered
Sep 2015  WG (rough) consensus on updates to RFC-4880.
Feb 2016  First WG I-D for RFC-4880bis
Jul 2016  RFC-4880bis WG I-D final call
RFC-4880bis goals

- Potential inclusion of curves recommended by the Crypto Forum Research Group (CFRG)
- A symmetric encryption mechanism that offers modern message integrity protection (AEAD)
- Revision of mandatory-to-implement algorithms and deprecation of weak algorithms
- An updated public-key fingerprint mechanism
Elliptic curve cryptography

- RFC-6637 specifies ECC for OpenPGP.
  - NIST curves,
  - but allows other curves (e.g. Brainpool).
- 2.1 implements this since 2011.
- NIST curves are somewhat suspect.
- We want curves with better repudiation:
  - ECDH with Curve25519,
  - EdDSA using Ed25519,
  - Maybe CFRG suggested curves
Elliptic curve cryptography

- RFC-6637 specifies ECC for OpenPGP.
  - NIST curves,
  - but allows other curves (e.g. Brainpool).
- 2.1 implements this since 2011.
- NIST curves are somewhat suspect.
- We want curves with better repudiation:
  - ECDH with Curve25519,
  - EdDSA using Ed25519,
  - Maybe CFRG suggested curves
Elliptic curve cryptography

- RFC-6637 specifies ECC for OpenPGP.
  - NIST curves,
  - but allows other curves (e.g. Brainpool).
- 2.1 implements this since 2011.
- NIST curves are somewhat suspect.
- We want curves with better repudiation:
  - ECDH with Curve25519,
  - EdDSA using Ed25519,
  - Maybe CFRG suggested curves
Elliptic curve cryptography

- RFC-6637 specifies ECC for OpenPGP.
  - NIST curves,
  - but allows other curves (e.g. Brainpool).
- 2.1 implements this since 2011.
- NIST curves are somewhat suspect.
- We want curves with better repudiation:
  - ECDH with Curve25519,
  - EdDSA using Ed25519,
  - Maybe CFRG suggested curves
Feature: Remote use

- We use ssh’s socket forwarding to
  - run gpg-agent on the "safe" box
  - run gpg on an "exposed" box (server)
- See --extra-socket, --browser-socket.
Feature: Remote use

- We use ssh’s socket forwarding to
  - run gpg-agent on the "safe" box
  - run gpg on an "exposed" box (server)
- See --extra-socket, --browser-socket.
Donations

- 5000 USD/month from the Linux Foundation for 2015
- ProPublica article in February ...
- We received ~300 KEUR in donations
  - Individual
  - Corporate (Stripe, FB)
- No donation campaign right now
  - Tax issues
  - Turning g10code into a non-profit
- We are lucky — other projects still suffer.
Donations

- 5000 USD/month from the Linux Foundation for 2015
- ProPublica article in February ...
- we received ~300 KEUR in donations
  - Individual
  - Corporate (Stripe, FB)
- No donation campaign right now
  - Tax issues
    - Turning g10code into a non-profit
- We are lucky — other projects still suffer.
Donations

- 5000 USD/month from the Linux Foundation for 2015
- ProPublica article in February...
- we received ~300 KEUR in donations
  - Individual
  - Corporate (Stripe, FB)
- No donation campaign right now
  - Tax issues
  - Turning g10code into a non-profit
- We are lucky — other projects still suffer.
Donations

- 5000 USD/month from the Linux Foundation for 2015
- ProPublica article in February ...
- we received ~300 KEUR in donations
  - Individual
  - Corporate (Stripe, FB)
- No donation campaign right now
  - Tax issues
    - Turning g10\textsuperscript{code} into a non-profit
- We are lucky — other projects still suffer.
Donations

- 5000 USD/month from the Linux Foundation for 2015
- ProPublica article in February . . .
- we received ~300 KEUR in donations
  - Individual
  - Corporate (Stripe, FB)
- No donation campaign right now
  - Tax issues
  - Turning g10\textsuperscript{code} into a non-profit
- We are lucky — other projects still suffer.
Donations

- 5000 USD/month from the Linux Foundation for 2015
- ProPublica article in February . . .
- we received ~300 KEUR in donations
  - Individual
  - Corporate (Stripe, FB)
- No donation campaign right now
  - Tax issues
  - Turning g10\text{code} into a non-profit
- We are lucky — other projects still suffer.
How we spend the donations

- Neal Walfield as second full time developer
- Yutaka Niibe does contractual work (e.g. smartcards, ECC)
- Kai Michaelis helps with Enigmail part time
- Me :-}
How we spend the donations

- Neal Walfield as second full time developer
- Yutaka Niibe does contractual work (e.g. smartcards, ECC)
- Kai Michaelis helps with Enigmail part time
- Me :-)
How we spend the donations

- Neal Walfield as second full time developer
- Yutaka Niibe does contractual work (e.g. smartcards, ECC)
- Kai Michaelis helps with Enigmail part time
- Me :-)

Past

Present

Future
How we spend the donations

- Neal Walfield as second full time developer
- Yutaka Niibe does contractual work (e.g. smartcards, ECC)
- Kai Michaelis helps with Enigmail part time
- Me :-)

GnuPG
Special thanks

- David Shaw
- Marcus Brinkmann
- Jussi Kivilinna
- Andre Heinecke
- Debian folks:
  - Andreas Metzler
  - Daniel Kahn Gilmor
  - Daniel Leidert
  - Eric Dorland
  - James Troup
  - Matthias Urlich
  - Thijs Kinkhorst
- Bug reporters, reviewers, testers, donors, ...
Outline

Past

Present

Future
Past

Thanks to Snowden, new demand for encryption

Gpg and Web-of-Trust are too hard
- Keysigning parties are for geeks

Present

New default focus:
- Mass surveillance (not targeted)
- Easy to use

Future

Still supporting targeted users
- Question of default options
Past Present Future

Vision

- Thanks to Snowden, new demand for encryption
- Gpg and Web-of-Trust are too hard
  - Keysigning parties are for geeks
- New default focus:
  - Mass surveillance (not targeted)
  - Easy to use
- Still supporting targeted users
  - Question of default options
Support for TOR and GNUnet

- All network access via a separate module
- New option `--enable-tor` to route everything over TOR
  - challenge: We need a torified resolver
- GNU Naming System (GNS).
Support for TOR and GNUnet

- All network access via a separate module
- New option --enable-tor to route everything over TOR
  - challenge: We need a torified resolver
- GNU Naming System (GNS).
Support for TOR and GNUnet

- All network access via a separate module
- New option --enable-tor to route everything over TOR
  - Challenge: We need a torified resolver
- GNU Naming System (GNS).
Definition
Trust On First Use: Secure Shell’s trust model

- There is a detailed plan for a TOFU design
- Will be available in 2.2
- Will eventually be the default trust model
Definition
Trust On First Use: Secure Shell’s trust model

- There is a detailed plan for a TOFU design
- Will be available in 2.2
- Will eventually be the default trust model
Tofu

Definition
Trust On First Use: Secure Shell’s trust model

- There is a detailed plan for a TOFU design
- Will be available in 2.2
- Will eventually be the default trust model
Tofu

Definition
Trust On First Use: Secure Shell’s trust model

- There is a detailed plan for a TOFU design
- Will be available in 2.2
- Will eventually be the default trust model
GPGME is a library to access gpg, gpgsm, and gpg-agent.

Planned features:

- Better integrated language bindings
- Support for new gpg features
- Run gpg as a co-process
  - signature verification
  - decryption
GPGME is a library to access gpg, gpgsm, and gpg-agent.

Planned features:

▶ Better integrated language bindings
▶ Support for new gpg features
▶ Run gpg as a co-process
  ● signature verification
  ● decryption
GnuPG release scheduling

- 1.4 releases as needed
  - No ECC support, though.
- 2.0 will reach end-of-life in December 2017.
  - No backport of ECC or other RFC-4880bis stuff.
- 2.1 will be replaced by 2.2 and declared as stable:
  - Release date: End of this year.
  - Support for Curve25519 encryption.
  - Support for some proposed RFC-4880bis features.
  - ECC key generation needs --expert temporarily.
- 2.3 for RFC-4880bis development
  - Certain features will be backported to 2.2
GnuPG release scheduling

- 1.4 releases as needed
  - No ECC support, though.

- 2.0 will reach end-of-life in December 2017.
  - No backport of ECC or other RFC-4880bis stuff.

- 2.1 will be replaced by 2.2 and declared as stable:
  - Release date: End of this year.
  - Support for Curve25519 encryption.
  - Support for some proposed RFC-4880bis features.
  - ECC key generation needs --expert temporarily.

- 2.3 for RFC-4880bis development
  - Certain features will be backported to 2.2
GnuPG release scheduling

- 1.4 releases as needed
  - No ECC support, though.
- 2.0 will reach end-of-life in December 2017.
  - No backport of ECC or other RFC-4880bis stuff.
- 2.1 will be replaced by 2.2 and declared as stable:
  - Release date: End of this year.
  - Support for Curve25519 encryption.
  - Support for some proposed RFC-4880bis features.
  - ECC key generation needs --expert temporarily.
- 2.3 for RFC-4880bis development
  - Certain features will be backported to 2.2
GnuPG release scheduling

- 1.4 releases as needed
  - No ECC support, though.
- 2.0 will reach end-of-life in December 2017.
  - No backport of ECC or other RFC-4880bis stuff.
- 2.1 will be replaced by 2.2 and declared as stable:
  - Release date: End of this year.
  - Support for Curve25519 encryption.
  - Support for some proposed RFC-4880bis features.
  - ECC key generation needs --expert temporarily.

- 2.3 for RFC-4880bis development
  - Certain features will be backported to 2.2
Summary

- 2.1/2.2 will soon be the standard version.
- Solid development team.
- Making mass surveillance expensive.

Thanks for attending.
Summary

- 2.1/2.2 will soon be the standard version.
- **Solid development team.**
- Making mass surveillance expensive.

Thanks for attending.

Slides are © 2015 The GnuPG Project, CC BY-SA 4.0.

Summary

- 2.1/2.2 will soon be the standard version.
- Solid development team.
- Making mass surveillance expensive.

Thanks for attending.

Slides are © 2015 The GnuPG Project, CC BY-SA 4.0.

Summary

- 2.1/2.2 will soon be the standard version.
- Solid development team.
- Making mass surveillance expensive.

Thanks for attending.

Slides are © 2015 The GnuPG Project, CC BY-SA 4.0.