State of End To End Encryption

Werner Koch

FSCONS 15 — Gothenburg
November 7, 2015

Outline

What is end to end encryption

- Wikipedia needs 100 words to explain E2EE.
- Shorter:

  All data exchange between the user operated devices is encrypted and optionally integrity protected.

- Needed for:
  - Mail
  - Chat
  - Phone

Why do we want to have this

- All encryption requires a private key.
- A (private) key must be protected.

- Servers are other people's machines.
- Servers are not trustworthy as a middleman.

Solution:

- Keys on a device under sole control of the user:
  - Desktop/laptop/phone memory.
  - Smartcard,

Why do we want to have this

- All encryption requires a private key.
- A (private) key must be protected.

- Servers are other people's machines.
- Servers are not trustworthy as a middleman.

Solution:

- Keys on a device under sole control of the user:
  - Desktop/laptop/phone memory.
  - Smartcard,

Why do we want to have this

- All encryption requires a private key.
- A (private) key must be protected.

- Servers are other people's machines.
- Servers are not trustworthy as a middleman.

Solution:

- Keys on a device under sole control of the user:
  - Desktop/laptop/phone memory.
  - Smartcard,

History

- Restricted transport media.
- Cipher rooms.
- Private code books (super-encryption).
- PGP-2.

Online vs. offline

Online (e.g. XMPP)

- An active network connection is required.
- Negotiation of features possible.
- Easy to update the protocol.
- Higher attack surface (e.g. no air-gap possible).

Offline (e.g. OpenPGP)

- No network required.
- E2EE may even be handled by courier.
- Very hard to update the protocol.
- Can be used for high security tasks.

Online vs. offline

Online (e.g. XMPP)

- An active network connection is required.
- Negotiation of features possible.
- Easy to update the protocol.
- Higher attack surface (e.g. no air-gap possible).

Offline (e.g. OpenPGP)

- No network required.
- E2EE may even be handled by courier.
- Very hard to update the protocol.
- Can be used for high security tasks.

Outline

Bugged systems

- Crypto AG devices since 1955.
- Software with 40 bit export restrictions.
  Example: Lotus Notes used 64 bit key but always leaked 26 (1997–2000).
- Microsoft's NSA key in 1999.
- RSA BSAFE's with NSA rigged RNG (2004–2013).

Failed systems 1

S/MIME

- Rarely seen requests for it since 2013.
- Seems to have lost all trust when used in the standard PKIX setting.
- Probably still fine in controlled infrastructures.

Failed systems 2

DE-Mail

- Central re-encrypt service with no connection to regular mail.
- Expensive (pay per mail).
- Federal commissioner for data protection demanded an additional end-to-end layer for sensitive data at the launch of the system.
- Extra OpenPGP layer is now possible.
- Citizens do not use it due to legal obligations.

More or less failed systems

Silent circle 

- Trustworthy developers.
- Not a store and forward system.
- Inspectable source code but
- relies on automated (binary) software updates.

Active projects 1

CaliOpen 

- Unified messaging system with crypto options.
- Revitalization of the multi-MTA times of a former Internet.

Enigmail

- Example of an encryption plugin for mailers.
- Probably the most used one.
- A lot of flaws because it is heavily understaffed.

Active projects 1

CaliOpen 

- Unified messaging system with crypto options.
- Revitalization of the multi-MTA times of a former Internet.

Enigmail

- Example of an encryption plugin for mailers.
- Probably the most used one.
- A lot of flaws because it is heavily understaffed.

Active projects 2

Google E2E 

- Smart project with a solid code base.
- Takes advantage of being run by a huge mail provider
- Will also be deployed using the same code base by Yahoo.
- Adoption by the majority of gmail users is questionable.

Keybase.io

- Identify proof through social networks.
- Do we really want that?

Active projects 2

Google E2E 

- Smart project with a solid code base.
- Takes advantage of being run by a huge mail provider
- Will also be deployed using the same code base by Yahoo.
- Adoption by the majority of gmail users is questionable.

Keybase.io

- Identify proof through social networks.
- Do we really want that?

Active projects 3

Mailpile

- Webmailer under own control.
- Encryption is a core component.
- Portable.
- Understaffed but not restricted by a business model.

Mailvelope

- Browser extension for OpenPGP.
- Used for Webmail.
- Problem: Storage of private keys.

Active projects 3

Mailpile

- Webmailer under own control.
- Encryption is a core component.
- Portable.
- Understaffed but not restricted by a business model.

Mailvelope

- Browser extension for OpenPGP.
- Used for Webmail.
- Problem: Storage of private keys.

Active projects 4

STEED

- Make crypto mostly invisble.
- Based on Tofu and existing protocols.
- Update of mail clients required.
- Public tender to implement that.

Whiteout

- Javascript mail client with encryption and key managment.
- Available for different platforms.
- Mailprovider with mailboxes and key infrastructure.
- Access to other keyserver is also possible.
- Problem: Storage of private keys.

Active projects 4

STEED 

- Make crypto mostly invisble.
- Based on Tofu and existing protocols.
- Update of mail clients required.
- Public tender to implement that.

Whiteout 

- Javascript mail client with encryption and key managment.
- Available for different platforms.
- Mailprovider with mailboxes and key infrastructure.
- Access to other keyserver is also possible.
- Problem: Storage of private keys.

Outline

Which systems will prevail

Business infrastructure

- ☒ Google E2E
- ☒ Whiteout
- ☐ CaliOpen

Tools for the web

- ☐ Mailvelope
- ☒ Mailpile

Classic home user tools

- ☒ Enigmail (with STEED)
- ☐ Keybase.io

Which systems will prevail

Business infrastructure

- ☒ Google E2E
- ☒ Whiteout
- ☐ CaliOpen

Tools for the web

- ☐ Mailvelope
- ☒ Mailpile

Classic home user tools

- ☒ Enigmail (with STEED)
- ☐ Keybase.io

Which systems will prevail

Business infrastructure

- ☒ Google E2E
- ☒ Whiteout
- ☐ CaliOpen

Tools for the web

- ☐ Mailvelope
- ☒ Mailpile

Classic home user tools

- ☒ Enigmail (with STEED)
- ☐ Keybase.io

Conclusion

- B2B mail will eventually move towards E2EE.
- Home users will use more encryption but not more than 20%.
- Pluggable devices (cf. Mailpile) have a chance to go mainstream.

The non-business driven projects need your support!

https://gnupg.org/ftp/blurbs/fscons15_state-of-e2e-encryption.org

GnuPG

Conclusion

- B2B mail will eventually move towards E2EE.
- Home users will use more encryption but not more than 20%.
- Pluggable devices (cf. Mailpile) have a chance to go mainstream.

The non-business driven projects need your support!

https://gnupg.org/ftp/blurbs/fscons15_state-of-e2e-encryption.org

Conclusion

- B2B mail will eventually move towards E2EE.
- Home users will use more encryption but not more than 20%.
- Pluggable devices (cf. Mailpile) have a chance to go mainstream.

The non-business driven projects need your support!

https://gnupg.org/ftp/blurbs/fscons15_state-of-e2e-encryption.org

GnuPG

Conclusion

- B2B mail will eventually move towards E2EE.
- Home users will use more encryption but not more than 20%.
- Pluggable devices (cf. Mailpile) have a chance to go mainstream.

The non-business driven projects need your support!

https://gnupg.org/ftp/blurbs/fscons15_state-of-e2e-encryption.org