Security Bootcamp

January 2015

Objective for today

- Understand why it's necessary to take minimum steps / provide options
- Send an encrypted e-mail / chat message
- Receive an encrypted e-mail / chat message
- Have a list of some other helpful tools to explore and recommend

Why we care

GCHQ

GCHQ captured emails of journalists from top international media

- Snowden files reveal emails of BBC, NY Times and more
- Agency includes investigative journalists on 'threat' list
- Editors call on Cameron to act against snooping on media

James Ball
@jamesrbuk

Monday 19 January 2015 15.04 GMT

Most popular
Obama says 'we are a strong family' in upbeat

It's not a "what if" anymore

What is confirmed

- Many governments regularly intercept unencrypted Internet traffic of all kinds
- US Government has intercepted "encrypted" communications from Facebook, Gmail, Skype, and more
- Telecom providers are regularly asked to hand over private user data (and usually comply). This has been happening for years.

World news
liberty central

How the US government secretly reads your email

Heather Brooke

Secret orders forcing Google and Sonic to release a WikiLeaks volunteer's email reveal the scale of US government snooping

Tuesday 11 October 2011 15.33 BST

Computer science researcher and WikiLeaks volunteer Jacob Appelbaum, in 2005; the US government used secret orders to compel Google and ISP Sonic to give up his personal email records. Photograph: Jacob

Security vs. Anonymity

- Anonymity on the Internet today is almost impossible; most activity leaves a digital trail
- Using a service like Tor (The Onion Router) can *help* to anonymize certain traffic, but users can still reveal their identity accidentally
- VPN services can help too, but you have to trust those services not to hand over your data when asked

Minimum effort

- We should endeavor to make it easy to figure out how to communicate with us securely
- We should clearly present the security risks in communicating with us, especially when it's about political activities, etc. (ideally, before we start communicating)
- We want to make a minimum effort to *proactively* help our network keep their communication secure

Tools

- Encrypted e-mail / anywhere messaging
- Encrypted phone conversations
- Encrypted “chat” options

Terminology: PGP

- Pretty Good Privacy (PGP) is the underlying implementation or standard of "Public Key Infrastructure" that much encrypted communication relies on.
- Typically, one doesn't use PGP directly.

Terminology: GPG

- GPG is an implementation of a PGP standard
- There are several applications that use GPG, like GPG Tools for OSX (https://gpgtools.org/)

GPG Suite

Everything you need to get started with secure communication and encrypting files in one simple package.

Use GPG Suite to encrypt, decrypt, sign and verify files or messages. Manage your GPG Keychain with a few simple clicks and experience the full power of GPG easier than ever before.

For OS X 10.10 Yosemite
Compatible back to OS X 10.6

Download GPG Suite

https://gpgtools.org/

GPG for Mail
is an open source plugin for Apple Mail. Encrypt, decrypt, sign and verify mails using OpenPGP with a few simple clicks.

GPG Keychain
is an open source application for Mac OS X. It allows you to manage your OpenPGP keys. Create and modify your keys and import the keys of your friends from a key server.

English | Deutsch

GPG 4WiN

About Gpg4win | Documentation | Community | Support | Donate

Download Gpg4win

Change History - Check integrity

News

2014-11-26

Gpg4win 2.2.3 released

2014-09-04

Gpg4win 2.2.2 released

2014-08-14

Gpg4win 2.2.2-beta released

Older messages in news archive.

Gpg4win - a secure solution...

... for file and email encryption. Gpg4win (GNU Privacy Guard for Windows) is Free Software and can be installed with just a few mouse clicks.

Windows / Outlook

THE ENIGMAIL PROJECT

OPENPGP EMAIL SECURITY FOR MOZILLA APPLICATIONS

Home | Download | Documentation | Support | News | Links

search

A simple interface for OpenPGP email security

Download

v1.7.2 for Mac OS X
on Thunderbird 31

Announcements

08/29/2014 — Enigmail v1.7.2 has been released

07/12/2014 — Enigmail v1.7 has been released

About Enigmail

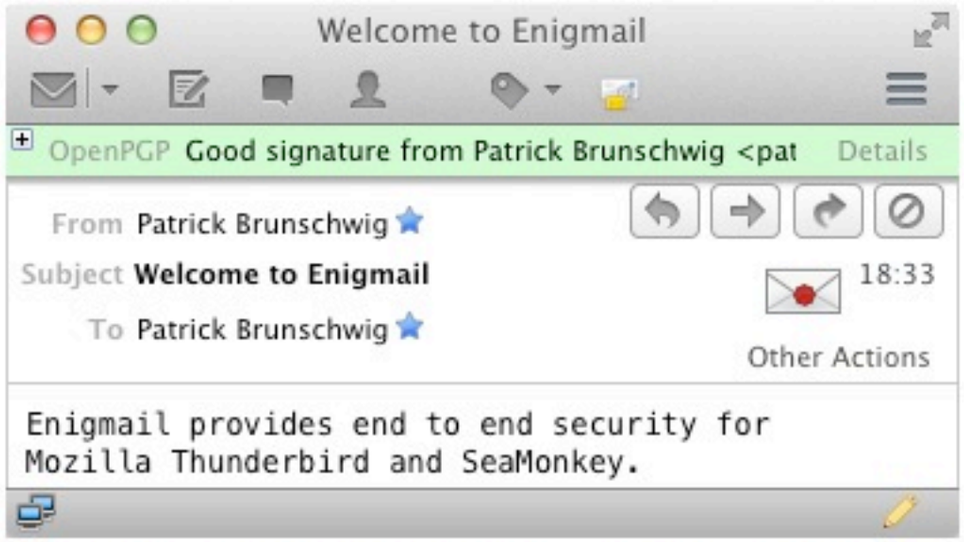
Features
Screenshots

What is this all about?

Enigmail is a security extension to Mozilla Thunderbird and Seamonkey. It enables you to write and receive email messages signed and/or encrypted with the OpenPGP standard.

Sending and receiving encrypted and digitally signed email is simple using Enigmail.

When starting it for the first time, you are guided through the basic setup. We also prepared a new users' guide that explains how to use OpenPGP.



Enigmail automatically decrypts and verifies your Email

Thunderbird: Windows, OSX, Linux

Keybase

- Is an attempt to make the process of getting started with public key encryption easier
- Is an attempt to use "social proofs" (social media profiles) as a way to verify identity, instead of requiring an offline verification (as was often done in the past)
- Most importantly: it's a good & easy way to publish your public key to the world
- Started by some very, very smart & trusted people (OKCupid!)

Encrypted e-mail on OSX

- Use GPT Tools / Suite and Mail.app
- Use EnigMail and Thunderbird

Encrypted e-mail on Windows

- Use GPG4Win and Outlook
- Use EnigMail and Thunderbird

Encrypted e-mail in the browser (Gmail)

- Encryption *in* the browser is a hard problem
- Google is working on this, but it's not ready for prime time...
- In the meantime, you can use your Keybase account to encrypt and decrypt messages in your browser that you can then send and receive in Gmail
- It's not a "smooth" experience, but it works

Encrypted e-mail on your mobile phone

- Phillip uses iPGMail (https://ipgmail.com/) on the iPhone. It works.
- I'm not up-to-speed on the latest options for Android, but I was using K-9 Mail with Android Privacy Guard without any issues

There are no excuses!

- You should be able to (most importantly) receive an encrypted message from a participant
- You should be able to respond with an encrypted message, or provide options for a way to securely communicate with you
- There are LOTS of options. No excuses.

Redphone/Signal

- Redphone provides encrypted voice calls on Android
- Signal provides encrypted voice calls on iOS devices
- These two programs can initiative / receive calls from each other
- They work in a pinch. Not perfect.

Chat Secure

- Think of it as SMS or iMessage
- Uses a different encryption scheme (OTR / Off-the-record)
- Theoretically works on iOS and Android
- It seems to be buggy / not very user friendly :(
- Blame Dave.
- We are now investigating Telegram. Stay tuned.

Other simple options

- One time secret, https://onetimesecret.com/
- 10-minute mail, http://10minutemail.com/10MinuteMail/index.html
- Cryptocat, https://crypto.cat/ (Simple encrypted chat for iOS, OSX, Chrome, Firefox, and Safari)

Further reading

- The most up-to-date resource available today is https://ssd.eff.org/en
- Most other resources are outdated or inaccurate
- Snowden's revelations obsoleted a lot of earlier thinking and guides

Now, let's do this!

- Go to http://bit.ly/brisingteam
- Pick a person from the list
- Find their public key
- Send them an encrypted message
- If you've received an encrypted message, decrypt it and read it out.

Adding your e-mail to your key

- One thing to note: Keybase doesn't automatically add your main e-mail address to your key
- So you'll need to do that manually, either using GPG Tools or using the `gpg` command line tool

GPG Keychain Access

New Import Export Undo

Type	Name	Email
pub	Jacob Appelbaum	error@debian.org
pub	James McClelland	jamie@mayfirst.org
pub	Jamie McClelland	jamie@mayfirst.org
pub	JayJay	artactivism@gn.apc.org
pub	Jeff Larson	jeff.larson@propublica.org
pub	Joseph Lorenzo Hall	joe@cdt.org
pub	Keybase.io Merkle Signing	merkle@keybase.io
pub	keybase.io/alexkelly	alexkelly@keybase.io
pub	keybase.io/brotherboyd	brotherboyd@keybase.io
pub	keybase.io/chrislaing	chrislaing@keybase.io
pub	keybase.io/cristianffff	cristianffff@keybase.io
pub	keybase.io/daveomitchell	daveomitchell@keybase.io
pub	keybase.io/dawn	dawn@keybase.io
pub	keybase.io/jessebrown	jessebrown@keybase.io
pub	keybase.io/kellan	kellan@keybase.io
pub	keybase.io/max	max@keybase.io
pub	keybase.io/moraviadelao	moraviadelao@keybase.io
pub	keybase.io/pippinlee	pippinlee@keybase.io
pub	keybase.io/possiblybob	possiblybob@keybase.io
pub	keybase.io/saleemkhan	saleemkhan@keybase.io
pub	keybase.io/shirleysquirrely	shirleysquirrely@keybase.io
pub	keybase.io/sorenwar	sorenwar@keybase.io
pub	keybase.io/timbunce	timbunce@keybase.io
pub	Laura Tribe	tribe.laura@gmail.com
pub	Luc Didry	luc@didry.org
pub	Mallory Knodel	mallory@mayfirst.org
pub	Marian Dörk	md@mariandoerk.de
pub	Michael Kreil	mail@michael-kreil.de

2014-01-28 2,048 RSA 00A4826E
2011-05-08 1,024 DSA 43D7E53B

112 of 112 keys listed

Key Inspector

Key | User IDs | Subkeys | Photos

Owner:
Name: keybase.io/brotherboyd
Email: brotherboyd@keybase.io
Comment:

Dates:
Created: 12 January, 2015 10:15 AM
Expires:

Key: Public key
Key ID: 08BBBF30179A7A0C
Length: 4,096
Algorithm: RSA
Fingerprint: 1BFE CC93 2A75 9BBC ADF7 5E75 08BB BF30 179A 7A0C
Validity: Unknown
Capabilities: esca

Other:
Ownertrust: Unknown
Disable
Change Passphrase Change Expiry Date

GPG Keychain Access

New Import Export Undo

Type	Name	Email
pub	Luc Didry	luc@didry.org
pub	Mallory Knodel	mallory@mayfirst.org
pub	Marian Dörk	md@mariandoerk.de
pub	Michael Kreil	mail@michael-kreil.de
pub	Michael P. Soulier	msoulier@digitaltorque.ca
pub	Michael Rogers	michael@briarproject.org
pub	Moris	delao.moravia@gmail.com
pub	Nat Meysenburg	nat@stealthisemail.com
pub	Nathan of Guardian	nathan@guardianproject.info
pub	Nina Reyes	nina@palantetech.com
pub	nulterm	
pub	Pat Hawks	pat@pathawks.com
pub	Paul Tagliamonte	paultag@debian.org
sec/pub	Phillip Smith	ps@phillipadsmith.com
sec/pub	**Phillip Smith**	**ps@phillipadsmith.com**
pub	Rebekah Wilce	rebekah@prwatch.org
pub	Ross Glover	ross@ross.mayfirst.org
pub	Scott Klein	scott.klein@propublica.org
pub	Shirley Wang	shirley@thepublicsociety.com
pub	Simon Loffler	simon.loffler@gmail.com
pub	Stuart Watt	stuart@morungos.com
pub	Taylor Buley	buley@outlook.com
pub	Thomas Gideon	cmdln@thecommandline.net
pub	Thomas Levine	_@thomaslevine.com
pub	Tim Groves	tim.m.groves@gmail.com

Double click your key

Key Inspector

Key | User IDs | Subkeys | Photos

Name	Email	Comment
Phillip Smith	ps@phillipadsmith.com	
Phillip Smith	phillipadsmith@keyb…	
Phillip Smith	phillipadsmith@gmai…	
PhotoID		

Click the + to add a new e-mail

Signatures:

	Name	ID	Created	Expires
sig 3	Phillip Smith	D63C5D49	2014-01…	

+ − Revoke

Continued...

- Then open your Terminal app (Applications > Utilities > Terminal)
- Then type `keybase push -u`
- That's it! Now people can send encrypted e-mail to your main e-mail address easily
- If you need to use the gpg command-line tool, ping Phillip on Skype for help

Security Bootcamp

January 2015