LINUX VOICE TUTORIAL

KEEP MESSAGES SECURE WITH PGP

BEN EVERARD

The Feds (and GCHQ, and the NSA) are snooping on our communications, but we can fight back with encryption

Normal email is one of the least secure forms of communication available – less secure even than post cards. These mails can typically be read by anyone on the same network as you, anyone at the ISP, anyone at your mail provider, anyone at the recipient's ISP and anyone on the same network as the recipient, as well as anyone with access to the various networks between the two ISPs.

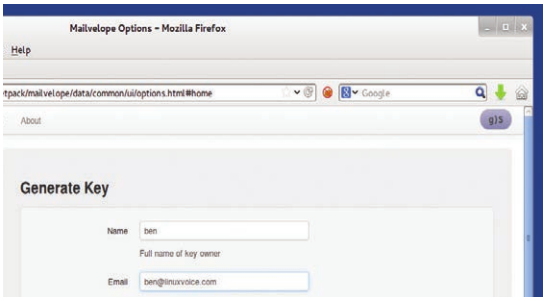
If you use SSL or TLS to connect to your inbox, then it improves things a little, but it's still vulnerable as soon as it leaves your mail provider.

PGP (Pretty Good Privacy) is a program designed to remove these weaknesses. It uses the normal email system, but adds a layer of encryption to protect them in transit. These days, PGP is usually used to refer to the OpenPGP format for these encrypted messages, rather than the PGP program specifically.

The OpenPGP format uses two different types of encryption: symmetric key and public key. In symmetric key encryption the same key (basically just a binary string that's used as a password) is used to encrypt and decrypt the message. In public key encryption, two different keys are used (one to encrypt and one to decrypt). The phrase 'private key' can refer to either the key in symmetric encryption, or the secret key in public key encryption. To avoid this ambiguity, we won't use the phrase in this article, but you may come across it in software.

When encrypting a message with an OpenPGP-compatible program, the software generates a random symmetric key and encrypts the text. This ciphertext forms the bulk of the message.

The problem is that the recipient of the message has to know the key, but it can't be included in the message otherwise anyone who intercepts the message will be able to read it. This is where public key encryption comes into play. Everyone who uses PGP first creates a public/secret key pair. The public key is made public while the secret key is known only to the user. However, anything encrypted with the public key can be decrypted only with the secret key and visa versa.



The colour and message in the top-right corner are a random security code so you can distinguish real Mailvelope messages from spoofs.

Public and private keys

The solution is to encrypt the key for the message with the recipient's public key. When they receive the message, they can then decrypt the key for the message, and then decrypt the message itself. This is a bit convoluted, but it's much less processor-intensive than encrypting the whole message using public key encryption.

You can use OpenPGP in most mail clients, but we'll look at doing it in webmail. Since OpenPGP is purely a text format, you could generate the encrypted message elsewhere and copy and paste it into your email. That's exactly what we'll do, but instead of copy and paste, we'll use a browser extension to convert the plaintext to encrypted ciphertext.

Mailvelope (**www.mailvelope.com**) works with Chrome/Chromium and Firefox, and it comes pre-configured to work with some of the most popular webmail providers (Gmail, Yahoo, Outlook.com and GMX). Installing it is no more challenging than downloading the extension from its Releases section (**https://github.com/toberndo/mailvelope/releases**) and opening the file with the appropriate web browser.

The first step is to generate a public/secret key pair. In Chrome/Chromium, you can get to this by clicking on the padlock icon that should have appeared to the right of the address bar. In Firefox, this options menu is a little more hidden. First, you'll need to go to view

USING OTHER MAIL CLIENTS

We've described the process for working with Mailvelope, but the process is almost identical for all OpenPGP-compliant software. You shouldn't have any problems following along using Thunderbird or Evolution, or even AGP and K9 for Android or Cyanogenmod.

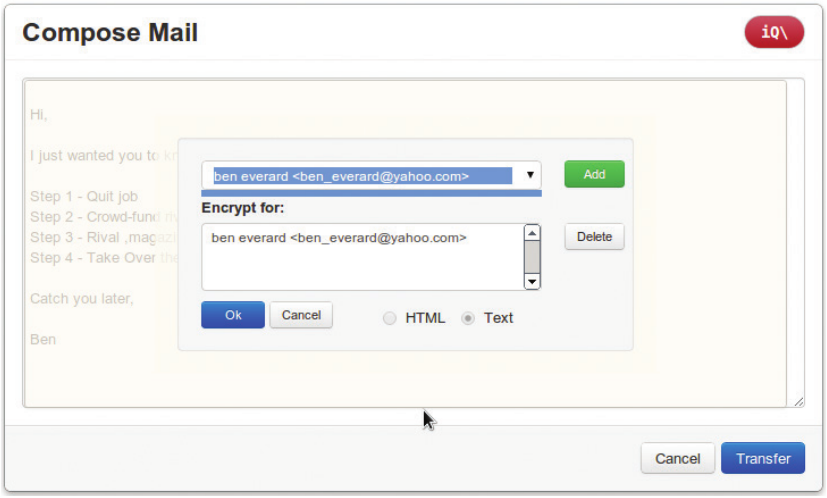
Regardless of the software, you'll still have to go through the same process of generating and exchanging keys before you can communicate with someone. As mentioned in the main text, you should be able to transfer keys between these pieces of software so you can access the same mail account through different programs.

Mailpile is a mail client designed to bring PGP to the masses by making it easier to set up OpenPGP encryption, even for new users. The project raised just over $163,000 in crowdfunding and is currently in development, and you can track its progress at **www.mailpile.is**.

DIGITAL SIGNING

OpenPGP encryption ensures that only the intended recipient can read the message; however, it doesn't guarantee that they receive the message, or prove who sent the message. Encryption can't help with the first of these, but there is something you can do about the latter measure.

In many OpenPGP mail clients (and the **gpg** command line tool), you can add a digital signature to a clear-text message. It does this by leaving the message in plain text, but also encrypting a hash of the message with your secret key. This encrypted hash is known as a digital signature. Since it's encrypted with your secret key, it can be decrypted with your public key. Any recipient that knows your public key can then decrypt this hash and check it against the message. If they match, the recipient knows that it really came from you.



You can send encrypted messages to several people at once, and Mailvelope encrypts it for each of them.

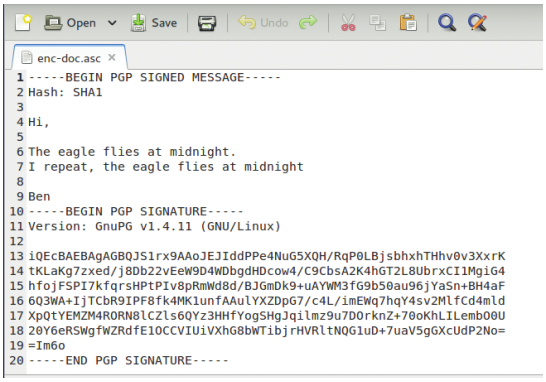
> Toolbars > Add-on bar. This will make the Add-on bar appear at the bottom of the screen, and then you should find the padlock icon on the right-hand side of this. This icon will bring up a menu, and you'll need to select Options (see the image, left).

In the Options screen, you can create a new public/secret (private) key pair by selecting Generate Keys. Once you've done this, you can go to the Display Keys screen to see it. This screen will show all the keys that Mailvelope knows, whether they're other people's public keys or your own public/secret key pairs.

Before you can receive emails, you have to send your key to the people you want to communicate with. The key file can be exported from the Display Keys screen (you can also export your public/private key pair here and import them into another mail program).

Getting the public key to the recipient can be a challenge. The best way to do this is to physically transport the key, as you can be completely sure that they got it correctly. The easiest way is just to email them the keyfile. However, it's possible for some malicious attacker to intercept this message and change the keyfile.

There are two other options: key servers and webs of trust. Key servers are databases of keys that you can add your keys to, and retrieve other people's keys from. For example, try **http://keyserver.pgp.com**



You can use gpg to create signed documents from the command line. Just run gpg --clear-sign <text-file> to generate a file containing the plain text and a signature.

or **http://pgp.mit.edu**. Of course, it is possible that some attacker could take control of one or more of these key servers and put fake keys in them. Webs of trust have a decentralised method of verifying keys. It's done by people digitally signing the keys of people they've met and exchanged keys with. If you need to communicate with someone, you can then tap into this web of trust and see who trusts them. Perhaps someone you trust also trusts them. Perhaps someone you trust trusts someone who trusts them. If this chain is short enough, then you can be confident that you can trust the person. Unfortunately, Mailvelope doesn't currently support webs of trust.

Keep it secret, keep it safe

As is so often the case, the decision on which way to distribute your key comes down to security versus convenience. If you're concerned, you could always follow up with another method such as a phone call to confirm the key. Once someone has sent you their key, you just need to load it into Mailvelope using the Import Keys screen in the Options.

Getting set up with keys is the hardest (or at least, most inconvenient) part of using any OpenPGP-based communication. Once you've done this, it's easy. With the Mailvelope extension running, just use your mail provider's web page as normal (if your mail provider isn't already on the Mailvelope watch list, you'll need to add it in the Options). When you get to the compose page, you'll see a floating icon of a pen and paper. Click on this and it will open a new window to let you enter the text for the message. Once you've written the message, click on the padlock, and add one or more people to the list that it's encrypted for, then Transfer to put the ciphertext into the email.

If you receive an encrypted message, Mailvelope will display a decrypt icon; click on this to enter the passphrase you entered when you generated the key. This password gives you some security even if an attacker gets access to your machine.

Provided you exchange keys securely, and keep your keys safe, OpenPGP provides security that is thought to be unbreakable with current technology.