Mailvelope for Email Encryption

Steve Revilak
https://masspirates.org/blog/category/cryptoparty/

Cryptoparty @ Somerville Public Library

July 15, 2016

What is Mailvelope

- Mailvelope is a browser extension (for Chrome and Firefox)
- It allows you to do end-to-end email encryption, using popular webmail systems.
- You can get it from `https://www.mailvelope.com/`
- Mailvelope's encryption is based on PGP (via OpenPGP.js)

What is end-to-end email encryption

- It's encryption for email
- End-to-end means "only the person(s) you're communicating with will be able to read your messages"
- In particular, the folks who run your webmail service *will not* be able to read your messages

What is (Open)PGP

- PGP = Pretty Good Privacy.
- OpenPGP = the standard behind PGP. It's a standard for data encryption and digital signatures.
- OpenPGP.js (which mailvelope uses) is an implementation of the OpenPGP standard.
- GnuPG (aka, the GNU Privacy Guard) is another OpenPGP implementation. (But it's not what we're focusing on today.)

Encryption Keys

- Like most encryption tools, Mailvelope (and PGP) are based on *keys*.
- *Private Key*. A very big number. Private keys are used to decrypt messages. It's a secret; keep it to yourself.
- *Public Key*. Public keys are used to encrypt messages. They're public; give them out freely.

cleartext $\rightarrow$ public key $\rightarrow$ encrypted message
encrypted message $\rightarrow$ private key $\rightarrow$ cleartext

Let's get Started!

- Install mailvelope, restart browser
- Click "Mailvelope" icon
- Options $\rightarrow$ Key Management $\rightarrow$ Setup
  - Generate Key

(If you already have a key, click "Import Key" instead of "Generate key")

Generate Key

- Provide your name (or, as much of your name as you want)
- Provide your email address
- Provide a password. **DO NOT FORGET YOUR PASSWORD**.
- Uncheck "Upload public key to Mailvelope Key Server" if you're not ready to do this yet.
  - Once you upload a key to a keyserver, you can't delete it. You can only revoke it.

It might take Mailvelope a few minutes to generate your key.

What does my key look like?

- Mailvelope → Key Management → Display Keys.
  - Locate your "primary" key, and click the key's "info" button.
  - Click "Export", then "Public". You should see `BEGIN PGP PUBLIC KEY BLOCK`
  - Click "Save" to save your public key as a file.

While we're here, it's probably a good idea to save a copy of your private key (as a backup).

Exchange Public Keys (1)

- Say "hi" to the person sitting next to you. :)
- Locate `Test_pub.asc` – this is the public key you saved earlier.
- Attach `Test_pub.asc` to an email message, and send it to the person sitting next to you.

Question: are there any risks in sending a public key via email?

Exchanging Public Keys (2)

- When you get your friends `Test_pub.asc`, save it to a file (probably a good idea to change the name when you save it).
- Mailvelope $\rightarrow$ Import Keys $\rightarrow$ Import key from file

Now, go to Key Management $\rightarrow$ Display keys. You should see your buddy's key.

Send an encrypted Message

- Compose a new email message to your buddy
- Click mailvelope's "external editor" button
- Write your email in the external editor
- Click "Encrypt"

Notice the alphabet soup? That's an encrypted message. This is all your email provider sees.

- When you receive your buddy's message, click mailvelope's "Locked Envelope" icon.
- Provide the password to unlock your key.
- Mailvelope shows you the message cleartext (i.e., the decrypted message)

What's a keyserver?

- A keyserver is a directory where you can look up keys (e.g., the key of a person you want to send an encrypted message to).
- When you're comfortable using your key, it's okay to upload it to a keyserver. This will make it easier for others to find.
- Key Management $\rightarrow$ Import Keys provides a way to look up keys using a keyserver

Playtime!

Send a few more encrypted messages, for practice

Questions for Discussion

- Did anyone receive a message with a signature at the bottom? Was the signature encrypted?
- Suppose you attached a file to your encrypted message – will the file be encrypted? If not, how could you encrypt the file?
- Remember the "Encrypt" button (you clicked this when you were done composing an email message). There's also a "Sign" button – what does "Sign" do?

Coda

- If you like mailvelope and wind up using it, please consider making a donation to `https://www.mailvelope.com`.
  - The same holds for any other Free Software that you use.
- Any questions?