Encrypted email with Thunderbird

Tom Ryder

tom@sanctum.geek.nz
https://sanctum.geek.nz/

Why encrypt?

Because email is *inherently insecure*.

- Usually passes through several untrusted public networks
- Usually in plain text
- If it's encrypted, it's normally in transit and with third-party keys that might be compromised
- Subject to filtering, logging, tracking, and all sorts of nasties
- One of the NSA's biggest sources of information for PRISM

Always assume your plaintext email is being stored and analysed, because it *probably is*.

Does it work?

> “Encryption works. Properly implemented strong crypto systems are one of the few things that you can rely on.”
>
> — Edward Snowden

- Email providers *cannot do this for you*; they might be compelled to surrender crypto keys:
  - LavaBit
  - Silent Circle
- OTR (Off-The-Record) is the equivalent system for instant messaging; can present about this too if there's interest

What's encrypted?

Only the *contents* of the email, including attachments.

- Not its subject line!
- Not the date it was sent!
- Neither the sender nor the recipient addresses!
- Not the software used to send it!
- Not the IP address of the sender mail agent!

If you want this metadata to be secret as well, you need an anonymous email service that you use over Tor.

Can I use Gmail/Hotmail/Live Mail?

- **Sort of.**
- You can't really use a mail web interface without a lot of hassle.
- If your provider offers IMAP/POP/SMTP support, however, everything should work fine.
- Set it up in Thunderbird and you're good to go.

What to encrypt?

All your private communication, ideally!

- **TNO – Trust No One**
- **EFE – Encrypt [Frickin'] Everything**

- Your messages can't be parsed to build a marketing profile on you or target ads to you.
- Your messages can't be decrypted by the NSA or other intelligence agencies (as far as we know!)
- Your messages are essentially useless to everyday attackers who compromise your email account or provider.

Everything?

Yes. It's mostly a political move:

- **If a large number of people use encryption for everyday things, it legitimises encryption and makes it harder for governments to ban it.**
- Otherwise it runs the risk of being seen only as a tool for nerds, paranoids, and criminals, rather than a way for everyone to exercise our right to privacy. This is PGP's single biggest problem.
- The NSA tried to legally circumvent encryption in the 90s, limiting key size and software exports. They may try it again.

How does it work?

- You generate a **keypair** on your machine; one private key, and one public key.
- The **private key** *never leaves your machine*.
- The **public key** can be given to all your correspondents, and published on the internet safely. It includes your email address, and should include your real name.
- People *encrypt* messages to you with your **public key**, which you can then decrypt with your **private key**.
- You can also *sign* messages with your **private key**, which people can verify against your **public key**.

Installation

- On Ubuntu and derivatives:

```
# apt-get install thunderbird enigmail
```

- On Debian:

```
# apt-get install icedove enigmail
```

Demonstration

- **Thunderbird/Icedove**, the email software
- **Enigmail**, the email encryption plugin
- **Mutt**, a console-based email program, on the other end

Debian Wheezy 7.0 with XFCE

Public key distribution

- Your public key is designed for distribution; advertise it with pride!
- Use keyservers; NZRS maintains one: `pgp.net.nz`.
- Ask new correspondents for their public key, especially technical people.
- You decide how much you trust your keys; best way is to meet up in person and trade keys.
- If you send automatic email to your customers, offer to encrypt the mail you send them; let them upload their public key to your service.

Tom's public key

FA09 C06E 1B67 0CD0 B2F5 DE60
C142 86EA 77BB 8872

Thomas Ryder (tyrmored, tejr)

tom@sanctum.geek.nz
https://sanctum.geek.nz/keys/pgp/tom@sanctum.geek.nz.pub.asc

- Sign and encrypt messages to me
- Attach your public key
- I'll reply telling you if the encryption worked

Questions?

Happy to demonstrate any part of my own setup if at all helpful.

- Pretty Good Privacy — https://en.wikipedia.org/wiki/Pretty_Good_Privacy
- GnuPG — https://www.gnupg.org/
- Linux Crypto: Email — https://sanctum.geek.nz/arabesque/linux-crypto-email/

Any interest in a presentation about OTR (Off-The-Record) Encryption for instant messaging? Easier than PGP!