Dip a toe in crypto (aka encryption and GnuPG)

Zak Rogoff & Steve Revilak

Encryption and Bicycle Riding

Who here knows how to ride a bicycle?

- It took practice
- You may have fallen down a few times
- It was easy, once you got the hang of it
- Anyone can do it!

Learning encryption is like learning to ride a bike.

What is encryption?

- Encryption - the process of encoding data, such that only the intended recipient(s) can read it.

Related to encryption:

- Integrity - being able verify that a piece of data is hasn't been modified.
- Non-repudiation - being able to identify the party who authored the data.

Who cares about encryption?

- Whistleblowers, activists, law enforcement, doctors, lawyers, merchants, financial institutions, journalists, researchers
- Anyone who uses electronic communications
- Anyone with a portable computer (e.g., laptop, cell phone)
- Anyone who stores data with a third party
- The government (who doesn't want you to use it)

Patent Trolls, Email, & Discovery

I first became interested in GnuPG for message signing

- I worked for a web company
- We were sued by a patent troll
- Turned over ~ 23,000 emails during discovery
- If my email ever becomes "evidence" in court, I want to be sure it's what I actually said.

What is GnuPG?

GnuPG is a free software implementation of the OpenPGP standard.

- PGP stands for *Pretty Good Privacy*

PGP is a system for *encrypting* data, and for creating digital signatures (aka *signing*).

Commonly used for Email, but can be used with any type of data or file.

A brief introduction to keys

Alice wants to (securely) send a file to Bob.

- Alice encrypts the file with a password
- Alice sends the encrypted file to Bob
- Bob gets the encrypted file, but
- How does Alice (securely) get the *password* to Bob?

This is the dilemma with password-based encryption.

Public key cryptography avoids this problem entirely. Instead of passwords, you use public and private keys.

Public and Private Keys

In order to use PGP, you'll need a *key*. Keys exist as a pair, called a *keypair*.

- There's a *public key*. You share this with everyone (because it's public).
- There's a *private key*, (aka *secret key*). Don't share this with anyone (because it's a secret).

The private key can undo what the public key does, and vice versa; think of them as inverse functions.

A public key encrypts a message, and the corresponding private key decrypts it.

Public and Private Keys (2)

With keys,

- Alice encrypts the file with Bob's public key.
- Bob decrypts the file with his private key.

No need for a password!

What can you do with a key?

Signing

- Guarantees that a message was sent by someone with a particular private key (*and* wasn't subsequently altered).

Encryption

- Ensures that a message is readable only by someone possessing a specific private key.

Equations!?! Oh NOES!

decrypt(PRIVKEY, encrypt(PUBKEY, MSG)) = MSG

- This is how encryption and decryption works

decrypt(PUBKEY, encrypt(PRIVKEY, MSG)) = MSG

- This is how signing and verification works

The Many Uses of GnuPG

We'll focus on email today, but GnuPG has many uses.

- Encrypting sensitive files
- Verifying software downloads (.sig files)
- Encrypting your backups (esp. remote backups)
- Your package manager

It's vital that encryption software be free!

Email self-defense

https://emailselfdefense.fsf.org

Test Message

- Send an unencrypted message to edward-en@fsf.org, with your public key attached
- Download steve@srevilak.net's key, and send him an encrypted message. Fingerprint

  6F09 15FF 59CE E093 56F4

  BEEC E772 7C56 28C2 A300

GnuPG Wrapup

- PGP protects your privacy through encryption.
- provides non-repudiation through digital signatures.
- PGP is something that you can (and should!) use every day.
- GnuPG is a free software implementation of a public standard.

It's harder to backdoor software when the source code is public.

Resources

- GnuPG: http://gnupg.org/
- Riseup.net's Best practices for OpenPGP: https://help.riseup.net/en/security/message-security/openpgp/best-practices
- Cryptoparty handbook: https://www.cryptoparty.in/documentation/handbook
- Surveillance Self-Defense: https://ssd.eff.org/
- Email Self-Defense: https://emailselfdefense.fsf.org/