Digital Privacy

Troy Sankey

2014-02-08
Why I'm doing this

- Because I’m selfish.
- Because I’m selfless.
What I’m not here to talk about

- Whether somebody is really listening. For me, the argument stops at “they can”.
- Whether you should care that they are listening. I’ll assume you do care since you’re here.
- How to avoid some specific $SECRET_AGENCY. I prefer general solutions that work everywhere, all the time.
The Problem
Patriot Act (2001)

- legalized wiretapping. Email and telephone service providers can be forced to hand over any and all customer information. [1]
- infringes people’s freedom of association
A lot of our tasks have been offloaded to web services.

RMS proposes the term "Service as a Software Substitute" (SaaS). [2]

If you’re logged into Facebook, it uses browser cookies to track you even when you’re not at www.facebook.com.

Google...
Closed Source Software

- It’s difficult to figure out what closed-source software really does.
- We know that some closed source software records your communications while giving the false impression of privacy (Skype, Outlook Web App). [3]
- Some closed source software connects to license servers every time they are invoked. [4]
Cryptographic Software

- Cryptographic algorithms are hard to understand unless you are a mathematician. Not all encryption software is trustworthy, even if the author is benevolent.
- Some encryption software is even closed source...
Solutions
By "science" I am referring to the scientific method.
By "scientific method" I am referring to peer review.
By "peer review" I am referring to free and open source software (FOSS).
Off-The-Record Messaging

- OTR allows people to enter into an encrypted instant chat session using the OTR protocol and some personal questions.
- Uses end-to-end encryption (AES-256, D-H, SHA-1) and provides perfect forward secrecy and malleable encryption. [5]
- New questions are needed to start each new session, and the messages do not persist beyond the duration of the chat.
- Therefore, not suitable for email. We are willing to sacrifice some setup time if it means we can reduce the constant overhead...
Pretty Good Privacy

- PGP allows people to send private messages to each other using end-to-end encryption.
- Does not require that you trust your service provider. You only need to trust your peers.
- Not a perfect solution because it makes sending messages more complicated. Some PGP interfaces could be better optimized for beginners.
- GnuPG is the most common implementation of the PGP standard. In GNU/Linux, the program is called gpg.
Pretty Good Privacy (Diagram)

Alice

Bob's public key

Alice's private key

Combine keys

751A696C 24D97009

Alice and Bob's shared secret

Bob

Alice's public key

Combine keys

751A696C 24D97009

Alice and Bob's shared secret

Bob's private key

Alice's private key

Bob's public key
Package Signing and TLS

- Package signing helps guarantee that all the software on your computer is unmodified between you and your software vendor.
- Most GNU/Linux distributions will use PGP to cryptographically sign packages. For Example, Debian keeps a master PGP signing key to sign the Releases file for each repository. When you apt-get install foo it will automatically verify the signature. [6]
- TLS (e.g. https) is another (weaker) line of defense against man-in-the-middle attacks. This helps guarantee that all the software on your computer is unmodified between you and your software mirror.
Package Signing and TLS (in Debian)

- repository
- TLS
- Release.gpg
- GnuPG key
- GnuPG
- Release
- SHA256
- Sources
- SHA256
- Packages
- SHA256
- some_program.dsc
- SHA256
- gcc
- some_program.deb
Tor

- Tor, originally "The Onion Router".
- Anonymizes/obfuscates your IP address, thus your location, by using volunteer operated Tor relays to tunnel your IP packets.
- Used by people from oppressive countries where the government censors parts of the web.
- Also used by people that are aware that your American ISP logs everything you do, and hands over that information to the NSA (patriot act).
- catches:
  - no javascript.
  - slow
Tails is an operating system for the ultra-paranoid. [7]

- It integrates all of the technologies covered in this presentation, and enforces them.
- Runs off a liveUSB, and never saves anything. Think of it as incognito mode for your entire operating system.
Conclusion
- Use OTR to encrypt your instant messages
- Use PGP to encrypt your email, sign blog posts, install software, etc.
  - Stop using web mail, unless it’s your own physical mail server (unlikely) and you’re using TLS.
- Use Tor while browsing the web. Disable Javascript with the NoScript Firefox addon so Facebook won’t track your every move.
- I would just delete my Facebook account if I were you.
Prism-Break <https://prism-break.org/> is a very cool website to help you find alternative software that is secure and FOSS.
EAT PIZZA
SIGN KEYS

sha1:
920ede55d17d079f57300146e3c8e2a09172e0cc

sha256:
33b5915d6560367075fabd16635293557d3d47eaeade86852799369540d9b87e

References


Sassafras Software homepage. URL: http://www.sassafras.com/sassafras/.

References III


- Tails homepage. URL: https://tails.boum.org/.