Total Encryption

Teddy Hogeborn, Björn Påhlsson

2011-08-06

Slides

https://www.recompile.se/lectures/2011-08-06_Total_Encryption

Encryption

- Is security from eavesdroppers, it is **not** anonymity
- Anonymity is a whole other talk

A Question of Trust

Not covered in this talk

- Proprietary encryption

  "We're secure, don't you worry your little head!"
  Not verifiable - simple *claims* are not good enough
- Built-in solutions from proprietary OSes
  - A history of extremly inadequate security
  - Back doors and/or intentionally crippled security

Encryption uses **Keys**

- How do you know who you're talking to?
- Man-in-the-middle

- PKI - Public Key Infrastructure
  - Hierarchical - bad
    - X.509 (a.k.a. S/MIME for mail)
  - Web of trust - good
    - OpenPGP

      Most used: GnuPG (GPG)
    - Signing party

Mail

OpenPGP

- Thunderbird: Enigmail

  http://enigmail.mozdev.org/
- Outlook: Gpg4win/GpgOL

  http://www.gpg4win.org/
  (Outlook 2003 and 2007 only)
- Apple Mail: GPGTools/GPGMail

  http://www.gpgtools.org/gpgmail/
  (Right now OS X 10.6 or older)
- Configuring

  Make sure to configure to use SSL:
  - SSMTP, IMAPS, and POP3S
  - https://starttls.se/
  - http://mailcheck.iis.se/

Web mail?

- FireGPG http://getfiregpg.org/
  - **discontinued**
  - FireGPG on Firefox 5
    https://grepular.com/FireGPG_on_Firefox_5
- Various plugins - none use OpenPGP

Web browsing

Web Browsing & Web Apps

- Uses X.509 - unfortunately
- HTTPS
  - Only if the server supports it
  - Most *don't*
  - **Not core feature**
  - Opposite to site's purpose: to collect your data

Better than nothing

Web Browsing Using HTTPS

- Firefox: HTTPS Everywhere

  https://www.eff.org/https-everywhere
- Safari: SSL Everywhere

  http://safariextensions.org/detail/SSL_Everywhere/
  Precompiled unavailable - user must compile
- Chrome
  (Limited support)
  - KB SSL Enforcer
  - Use HTTPS
- Opera: Redirect to HTTPS

  https://addons.opera.com/addons/extensions/details/redirect-to-https

Social Networking

(Including photo sharing, etc)

- Web apps - see web browsing
- Same caveat - dependent on server

Supporting HTTPS & cares about data secrecy

- Diaspora https://joindiaspora.com/
  - Pods http://podupti.me/

    Host your own

Microblogging

Also web app

- Identi.ca https://identi.ca/
  - Host your own

Files on Disk

GPG with interface

- GNU/Linux
- Windows
  - ZIP, RAR, etc.

    Encryption not core feature, history of bad security
  - Gpg4win/GpgEX http://www.gpg4win.org/

    (As of today, 32 bit only)
- MacOS X
  - GPGTools/GPGServices
    http://www.gpgtools.org/gpgservices/
- Truecrypt
  - Single files a bit of work, meant for whole disks

Whole Disk or USB Drive

- Truecrypt http://www.truecrypt.org/
  - + GNU/Linux, Windows, and MacOS
  - - Boot-time **only on Windows**
  - - Not the best choice on GNU/Linux
- LUKS - Linux Unifies Key Setup
  - + Standard and built-in on GNU/Linux
  - - Boot-time only on GNU/Linux
  - - Not on MacOS
  - (For Ubuntu, use the “text-mode” or “alternate” installer)
  - Use FreeOTFE to access on Windows

Network File Sharing

(Network drive or NAS, **not** P2P)
SFTP a.k.a SSH, OpenSSH, etc.

- \- Private key system
- \+ Very widely used
- Linux client: sshfs http://fuse.sourceforge.net/sshfs.html
- Windows server
  copssh http://www.itefix.no/i2/copssh
- Windows client
  - Swish http://www.swish-sftp.org/ (Still in alpha state)
  - FileZilla
    - no shell extension
- MacOS client
  - Macfusion http://macfusionapp.org/

Instant Messaging (IM) and phone (VOIP)

Encrypted *protocol*

- Mumble http://mumble.sourceforge.net/
  - \- Private protocol
  - \+ Popular in some circles
- Jitsi http://jitsi.org/
  - \+ Standard XMPP
    Same as Jabber, Google Talk, etc.

P2P File Sharing

- Nothing
- Use network encryption

Network Traffic Encryption

Depends completely on the endpoints - both must run the same. prq, for instance, offers only OpenVPN

- OpenVPN
  - + Common
  - + Relatively easy to set up
  - - Non-standard protocol
- IPsec
  - - Complex to set up
  - + Standard; built-in to in all OSes

Summary

- Install HTTPS Everywhere (or similar) for your browser
  - Switch to a better social networking and microblogging platform
- Encrypt your disks and USB drives
  - All of them - boot time-encryption!
- Switch to a better IM and VOIP protocol & software
- Get an OpenPGP key!
  - Encrypt your mail
    - When you have the recipient's key
    - Otherwise, at least **sign** your mail
    - Defense against alteration
  - Attend keysigning parties and get signatures
- Look into getting a VPN or IPsec tunnel to your local most-used services
- Slides: https://www.recompile.se/lectures/2011-08-06_Total_Encryption