Tails

Steve Revilak
http://www.srevilak.net/wiki/Talks

Cryptoparty @ General Assembly Boston

May 18, 2014

What is Tails?

- Tails is for “The Amnesic Incognito Live System”
- Obtainable from `https://tails.boum.org/`
- A “live” operating system; you place it on a DVD, USB drive, or SD card and boot from it.
- It’s a Debian Linux distribution, with tools to help protect privacy and anonymity.
- Works on standard Intel/AMD processors, regardless of the operating system you’re using.

Why use Tails?

- You care about privacy and/or anonymity.
- You have to use a public/shared computer, and you don't know what kind of malware's been installed on it.
- You're a whistleblower, and you're trying to hide from large governments.
- You're an ordinary person, and you don't want to be surveilled by terrorist governments.

Burning Tails

- You'll download an .iso image from `https://tails.boum.org`
- Ideally, you'll verify the integrity of the download the integrity of the download, as described in `https://tails.boum.org/download/index.en.html`
- Burn it to a DVD or USB.

Burning to a DVD ensures that the system never changes (i.e., no malware). Burning to a USB gives you some extra flexibility.

You can use Applications > Tails > Tails Installer to burn the installation to a USB.

Using a USB Disk with the DVD

- When the tails installation is on a DVD; it can't be modified. Tails looks exactly the same way at each boot. It's *amnesic*.
- In this configuration, tails uses RAM for storage, instead of a hard disk. The RAM is erased at shutdown. (again, it's *amnesic*).
- It's helpful to have a USB, for files that need to persist across reboots, or for files that you need to get to. For example, this slide presentation.

Applications > System Tools > Disk Utility makes it easy to encrypt a USB drive for use with Tails.

Tail’s Distinguishing Characteristics

- Most operating systems try to remember lots of things for you.
  - This is convenient, but it leaves lots of bread crumbs lying around on your computer.
  - Tails doesn’t want to leave a trail of breadcrumbs. It tries to remember as little as possible.
- Tails tries to Proxy all internet traffic over the Tor network.
  - This includes, but is not limited to the Tor Browser.
  - Instant messaging, mail is also sent over tor
  - Even command-line programs (ssh, wget) are configured to send traffic through Tor.

Let’s look at some of the tools that tail provides.

Web Browsing

- Iceweasel (the Debian version of Firefox) is the default web browser. It's configured to use Tor.
- "Unsafe Browser" is also Iceweasel, but it's configured *not* to use Tor.

Some Remarks about Browser Configuration

- Preferences > Privacy. By default, Tor will “Never Remember History”.
  - No more worries about persistent tracking cookies. They’re erased each time you close the browser.
- Another useful setting: save history, accept cookies (*not* third party cookies), and clear history when the browser closes.
  - This gives you essentially the same protection, but you can clear cookies/history in the middle of a session.
- Tor also comes with NoScript and HTTPS Everywhere.
  - NoScript blocks Java, Flash, Silverlight. Can also block javascript.
  - HTTPS everywhere tries to force https:// (instead of http://) whenever possible).

Pidgin

- Pidgin is an instant messaging and internet relay chat (IRC) client.
- I've found pidgin to work well with XMPP over Tor. I've had less luck with IRC. (But perhaps this is user error.)
- Pidgin also supports OTR – Off the Record Messaging.
- OTR generates a one-time encryption key. If someone were to "break" a one-time key, they'll get access to one session's worth of chats. Nothing before, and nothing after.

Let's try an XMPP demo (perhaps with OTR).

KeePass

Keepass is a password manager.

- Keepass stores username and passwords for different web sites and services.
- Keepass can generate (good) passwords for you
- Keepass allows you to copy and paste passwords, without having to view the password in clear text
- Passwords are stored in an encrypted file.

Your Keepass file has to be stored on a USB drive (or in persistent storage). Otherwise, it will disappear when you shut down tails.

Other Software

Aside from the security and privacy-enhancing software we've discussed, tails also includes:

- **Claws Mail**. A mail client (with good GnuPG integration)
- **Vidalia**. A control panel for Tor
- **A Virtual Keyboard**. For cases where you might have to worry about keystroke loggers.
- Lots of other useful software: GIMP, Inkscape, Open Office, Audacity.

Note: all of the programs we've looked at are Free software, and they'll work find outside of tails.

Caveats

There are some things I haven't figured out (and I'm sure there's some of user-error involved).

- Pidgin and IRC (as mentioned earlier).
- Some features won't work without a "Persistent Volume".
    - Examples: GnuPG, SSH keys, application preferences.
    - Persistent Volumes require tails to be installed on a USB or SD card. (You can use tails from a DVD, and have the persistent volume on a USB).
- MAC address spoofing is enabled by default. I've always had bad luck getting onto wireless networks with spoofed MAC addresses.

Conclusion

- Overall, Tails is a pretty neat distribution. Hopefully this will inspire more software to be “privacy conscious”.
- Tails has more security features enabled than your average operating system. But it’s still pretty usable.
- Try it. If you like it, consider making a donation to the project.