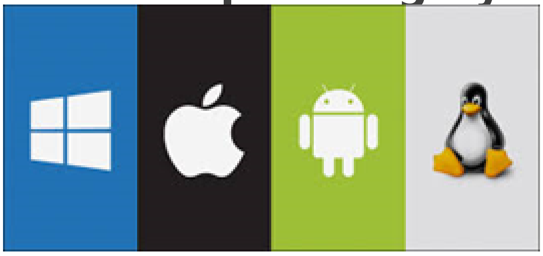
Security Best Practices - Part 4: Operating Systems

Travis - 2021-03-16 - Best Security Practices

Part 4: Operating Systems



TL/DR: Use a live system that specializes in security and privacy without sacrificing user productivity.

Staying anonymous on the Internet does not mean surfing the web securely. With the ever-increasing need to stay safe online as the risk of cyber-attack and NSA snooping increases, it is only fair that quite a few operating or distros as they are known, have gone down the lane of combining tools that should essentially help you remain anonymous.

Whilst there are three main operating systems, Windows, Mac & Linux, the main players are the closed source which means their code cannot be inspected for back doors or options to allow 3rd parties in, without your consent. Linux by nature is open source, allowing anybody to inspect and improve the code. As such it also allows for a more specific purpose, including privacy and security.

These privacy-centric Linux distros – although originally targeted at a niche crowd, have managed to be listed in a specific category under Linux distributions as the popularity and need for this has quickly ramped up over the years – and you now possibly have about 20 to choose from, however, there are certain versions which stand out as better than others

It is worth mentioning that some of the distribution comes with Tor’s solid anonymity network service built-in – which provides a rigid experience and allows you to play around the Internet anonymously. Some VPN providers may log your real IP address while still being able to see whatever data you may be transmitting at the point of exit of VPN servers, however, we at PIA are currently the only VPN provider who have been legally challenged on our no-logs policy. Other VPN providers state they do not log, however to date, there is no evidence to support this.

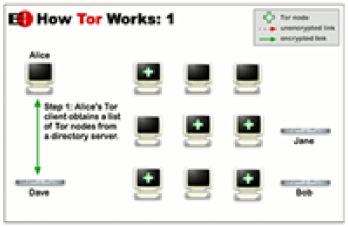
A VPN service still has a large number of advantages over the former which makes it somewhat superior in a way (depending on your personal situation), particularly general throughout (download) speed.

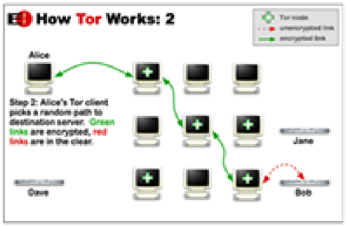
To give you an idea of how Tor’s anonymity network works, we’ll quickly give you a rundown before we go through (what I consider) the best security-centric distros out there.

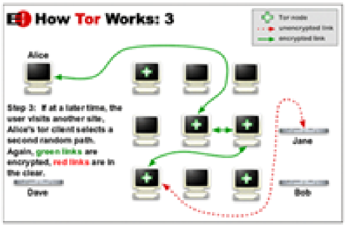
Understanding Tor

Tor is an acronym meaning 'The Onion Router', which refers to the standard layer of data encryption which was developed initially by the US Naval Research Laboratory in the 1990s and further developed by DARPA (Defense Advanced Research Projects Agency - Part of the US Department of Defense) as a way to protect US intelligence communications online.

Tor is an anonymity network that essentially works with nodes – that pretty much secures the network and provides the medium in which data is transmitted – through which every piece of data is re-encrypted multiple times as it passes through randomly selected nodes before reaching its destination as illustrated in the images below.


How Tor Works: 1
Tor node
unencrypted link
encrypted link
Alice
Step 1: Alice's Tor client obtains a list of Tor nodes from a directory server.
Jane
Dave
Bob


How Tor Works: 2
Tor node
unencrypted link
encrypted link
Alice
Step 2: Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.
Jane
Dave
Bob


How Tor Works: 3
Tor node
unencrypted link
encrypted link
Alice
Step 3: If at a later time, the user visits another site, Alice's tor client selects a second random path. Again, green links are encrypted, red links are in the clear.
Jane
Dave
Bob

Tor is also responsible for creating one of the most secure Linux distros out there – Tails – and also happens to be Edward Snowden's tool of choice.

Back to VPNs; as we mentioned above, the virtual private network services are usually premium and there’s no particularly free VPN network service out there. The quality of a VPN service really depends on the provider you sign up with; but generally speaking, VPN providers usually have servers in many locations all around the world and the connections are mostly fast, well-grounded when compared to Tor due to the continuous bounce of data from node to node.

Below we have analyzed the features of several different Distros. While just like with Browsers we understand that everyone has their preferred distro we are in no way trying to persuade you from choosing one over the other.

TAILS

- Developer: tails.boum.org
- Open Source: Yes
- Security: Excellent
- Privacy: Excellent

Background:
Depending on how paranoid you are or how crucial your need to remain unknown while on the Internet, the so-called TAILS tends to deliver on its promises. Its sole purpose is to ensure that you leave no digital footprint after you might have been done surfing the web – and it's unarguably one of the most used security-tailored Linux operating systems out there and also most likely the only one that has all its connections routed through the TOR anonymity network.

TAILS basically installs on a thumb drive and by default, all data is stored solely in RAM and completely erased when a TAILS session is exited.

The operating system is based on Debian and comes with a suite of open source tools that are specially meant for privacy-specific reasons. The OS also supports MAC address spoofing together with "windows camouflage" – that pretty much makes your usage of the OS go unnoticed.

User Interface:
TAILS is based on an archaic version of GNOME that is nothing short of ugly with a very minimalist-looking user interface that derails any possible chance of customization in regard to aesthetics and the general feel of the OS, there's also no standard way of saving files.

That, as important as it might be for some, is not too relevant in this case, most importantly, TAILS gets the job is done which is what you should mostly be concerned about. TAILS also has pretty good documentation and you can head on to their website to find out more.

Whonix

whonix
PRIVACY & ANONYMITY OS

- Developer: www.whonix.org
- Open Source: Yes
- Security: Excellent
- Privacy: Excellent

Background:
Whonix takes quite a different approach from those mentioned above as it's not a live system but instead runs in a VM – Virtualbox to be specific – where it is isolated from your main OS thereby minimizing the risk of DNS leakage or malware (with root privilege) infiltration – given that it runs in a virtual machine which is, of course, limited as it can get in regard the resources it can actually use.

Whonix consists of two parts – the first is "Whonix Gateway" which acts as a Tor gateway while the other is known as "Whonix Workstation" which is an entirely isolated network that routes all its connections through the Tor gateway.

Thereby utilizing two VMs which makes the entire OS experience pain sometimes (if you don't have powerful hardware) as you'll experience lags every now and then; however, it works effectively but not as secure as a live system – considering that you do not touch the system on your hard disk at all when using the likes of TAILS.

User Interface:
Whonix is based on Debian Linux but with a KDE desktop environment. Yet again, the OS is obviously not suitable for day-to-day use as you can only use it in a VM – sadly.

Qubes OS

QUBES OS
A REASONABLY SECURE OPERATING SYSTEM

- Developer: www.qubes-os.org
- Open Source: Yes

- Security: Excellent
- Privacy: Excellent

Background:
Qubes OS is yet another Edward Snowden tool of choice as he clearly revered Qubes OS during an interview with a technical journalist Micah Lee where the privacy advocate said that “I’m really excited about Qubes”.

Basically, Qubes aims to fix the shortcomings of the aforementioned distros – which mainly has to do with the poor or lacking user experience for day-to-day use while still combining the power of Whonix and Tor in one system.

Qubes approach to anonymity is what they call security by compartmentalization – which essentially means compartmentalizing “your digital life into securely isolated virtual machines (Vms)” – basically a simulated OS running in Qubes OS – in layman’s, an OS in an OS for pretty much any application you run.

Interestingly enough, the OS is the one shipping as default with Purism’s flagship Notebook PC that is supposedly presented as the most secure consumer PC – which is true in the rightful sense of it considering the powerful software and varying tools that come built-in.

User Interface:
So if you care so much for day to day usability without sacrificing functionality and the most apps you’d normally use, Qubes might just be your go-to security distro of choice that can be installed natively on your hard-drive compared to those listed above that are merely live systems – with the exception of Whonix of course.

UPR (Ubuntu Privacy Remix)

- Developer: www.privacy-cd.org
- Open Source: Yes
- Security: Excellent
- Privacy: Excellent

Background:
UPR is yet another installable security-centric distro that is particularly user-friendly and aims to provide an “isolated working environment where sensitive data can be dealt with safely.”

User Interface:
From the naming, you can easily tell that it’s based on Ubuntu and it happens to be the only one on this list using an Ubuntu base.

For what it's worth, the distribution is functional according to review on the internet and uses encrypted USB disks to store all your data to effectively protect it from unsolicited access. It also comes preinstalled with cryptographic tools such as TrueCrypt and GnuPG for encryption needs.

It is, however, worth noting that UPR is not necessarily designed for anonymous Internet use but it’s the second closest thing to a secure operating system if you’re looking to install on your PC rather than use a live system…..and you can, of course, install Tor or subscribe for a VPN service after you have it setup.

Conclusion
Considering TAILS is apparently the most prevalent of them all – at this time and it might as well be your safest bet, nonetheless, the rest of the distros we’ve mentioned above are likewise great and serve their purpose mostly – so now, it really does come down to personal preference.

For the sake of clarity and transparency, I personally use TAILS though I have yet to migrate to Qubes OS due to the more advanced user interface without compromise to security or privacy.

Tags

Security