The Red Spectre

07/01/24

Red Spectre Operations Security Manual

Table of Contents:

Introduction — What is Operations Security?

Operations Security (**OpSec**) is the process which identifies critical information in order to determine if friendly actions can be observed by enemy intelligence, determines if information obtained by adversaries could be interpreted to be useful to them, and then executes selected measures that eliminate or reduce adversary exploitation of friendly critical information.

Considerations for this must include a wide range of kinds of threats, both civilian and governmental ones.

Mass surveillance in capitalist states is used for the purposes of tracking radical activists and gaining information about them. Activists today are far more surveilled with the rise of modern technology — with tools such as IMSI catchers, drones, facial recognition software, and the pulling of location data from big tech and phone companies — without a warrant and

almost never because the target is believed to be a threat to peace. It is further claimed that true privacy does not exist or is unattainable, but this is not necessarily true and can be addressed through a combination of factors like good practices, media access controls, and the use of particular software and settings.

Proper and secure software, communication platforms, and so on will be the focus of this manual. For revolutionary communists everywhere, avoiding usage of insecure, corporate controlled platforms is nothing less than a requirement for both individual and organizational security.

1. Operating Systems

An **operating system** (**OS**) is, briefly, software which is installed on your computer to provide you with a way to interact with your computer’s hardware. This takes the form of running applications, managing computing functions, and so on. Without an OS present, your computer cannot be used.

There are many different operating systems available, most of which are mutually incompatible. The most widely used OS for desktop computers is Microsoft Windows, the most recent versions being Windows 10 and 11. The second most used is macOS, which is intended exclusively for computers produced by Apple Inc. (Macs).

Both Windows and macOS are *proprietary software*, which is to say that they are the exclusive property of a corporation (Microsoft or Apple Inc.). If the owing corporation wishes to put, for instance, telemetry and other invasive software into their OS, there is little anyone else can do to prevent it, even if these OSs are used by hundreds of millions people.

However, there are many viable alternatives to these proprietary operating systems, the most popular of which is **Linux**.

Linux (or GNU/Linux) is a kernel (the “core” of the OS) which forms the basis for many OSs, or *distributions*. Linux is, unlike Windows and macOS, free and open source software, meaning that it is free from proprietary ownership from a massive corporation, its contributors and developers are

people within the userbase itself, and most if not all of its source code is freely visible to the public. This means that any alternations to the code can be detected by the community, removed, and so forth if it decides that such a thing is needed.

Logo of Arch Linux, a popular distribution of Linux.

Converting from Windows or macOS to Linux is ***strongly recommended*** for members of The Red Spectre. Both Microsoft and macOS are megacorporations which are known to regularly collaborate with intelligence agencies controlled by the United States government, sell and otherwise provide personal information in massive amounts, place backdoors (purposeful security weak points) in their OSs, etc.

When bourgeois governments begin to enact more and more draconian measures against revolutionaries, it will be a certainty that they will reach out to these software corporations to provide

them with our personal information.

You must secure your system at all levels; even if you use a secure web browser, using an OS compromised with corporate spyware will nullify all of that.

1.1. Installing Linux

An installation medium with a storage capacity of at least a few gigabytes is strongly encouraged.

There are many different “flavors” of Linux available, all of which able to meet a vast pool of computing needs and desires. The most popular distributions include Arch, Ubuntu, Mint, Manjaro, Fedora, and many others. Mint, Ubuntu, and Manjaro are recommended for those new to Linux.

Regardless of the particular distribution, the installation process is generally uniform. This aspects of which will be briefly enumerated here:

1. Go to the website of the Linux distribution you would like to install (e.g. archlinux.org, linuxmint.com)

2. From the website, download a .iso file. This file is large as it contains most or all of what is needed to install the operating system.

3. Get an installation medium; an external device to store the operating system and be inserted into your computer. This can be a USB flash drive or writable optical disc (CD or preferably DVD).

4. Use a program such as balenaEtcher (etcher.balena.io) to flash the .iso file to the installation medium. If using an optical disc, use other software to burn it.

5. Store your personal files somewhere else, on another physical storage device, on a cloud storage provider, etc.

6. Access the boot menu on your computer, generally done via turning it off, pressing a key combination at startup with the installation

medium attached, and selecting the installation medium to boot from. The particular details of how to access your device's boot menu differs based upon your computer manufacturer.

7. Once you are booting from your installation medium, most of the aspects should become intuitive from then on. On Linux Mint, for example, you will be presented with an easily-understood graphical installer. On Arch Linux, everything with the installation is premised off a command-line interface (CLI). On more *esoteric* distributions such as Arch, please consult relevant resources for the details of installation, such as the Arch Wiki (wiki.archlinux.org).

8. Hopefully, your installation will be successful and you are now using Linux. You have secured a far greater level of privacy and security relative to Windows, for example.

2. Web browsers

A **web browser** is what is used to view pages and other content on the internet. Likely, you are using a

web browser to view this manual currently.

Similar to operating systems, proprietary, corporate web browsers dominate, with Google Chrome and Apple’s Safari being the most used browsers.

Also like operating systems, however, is that free, open source, and privacy-respecting web browsers are available and easily found.

Some of these include:

- LibreWolf (librewolf.net)
- ungoogled-chromium (github.com/ungoogled-software/ungoogled-chromium)
- GNU IceCat (www.gnu.org/software/gnuzilla)

Other web browsers, like Firefox, are viable, but have major issues such as including spyware. A guide for hardening Firefox may be found here.

2.1 Browser extensions

Several recommended browser extensions for further privacy and security are:

- uMatrix: blocks out things like scripts and cookies unless you specifically specify which ones you want enabled and on what level of a domain you want it enabled on (for instance, you can enable a certain script either only on the subdomain www.example.com, or only everything on the domain example.com, or everything contained by the top-level domain.com.

- uBlock Origin: filters content, largely advertisements that can track your activity across the internet. (Note: This extension is included in LibreWolf by default)

- Cookie AutoDelete: deletes unused cookies upon tab close, however may be configured in many different ways. Has support for whitelists and greylists.

- User-Agent Switcher: randomizes your user agent, which reports to websites what kind of operating system and web browser you use.

- LibRedirect: automatically redirects requests for popular websites (YouTube, etc.) to privacy-respecting alternatives (Invidious, etc.)

2.2 Search engines

Avoid privacy-invasive search engines such as Google (google.com). Instead, make your default search engine DuckDuckGo (duckduckgo.com), Startpage (startpage.com), searx-ng, and others.

3. Communication

Communication software is dominated by corporate spyware — platforms such as Discord are horribly insecure and will attempt to gather as much personal information about you as possible.

As such, communists need other, secure platforms to communicate. The most viable alternative to Discord are platforms which use the Matrix (matrix.org) protocol, most notably Element (element.io). Element is free, fully encrypted, and trivial to adjust to for those who have already used other instant messaging programs such as Discord.

3.1. Email

Email is a commonly used medium, yet many email providers such as Gmail, Outlook, and Yahoo Mail are extremely compromised and invasive.

Where email is used, platforms such as Proton Mail (mail.proton.me) or Tuta (tuta.com) should be used instead. Further, always use OpenPGP/GPG for encrypting your emails. Email, however, was a format never intended for privacy and therefore other communication mediums should be used instead when possible.

4. VPNs and Tor

Virtual private networks (**VPNs**) and **Tor** can be very useful for the purposes of anonymity, however, you must be mindful of the VPN provider in question. Proton VPN (protonvpn.com), for instance, offers a workable free plan and there are no major instances of data leaks for Proton VPN users.

Other VPN providers, however, are known to collaborate with state agencies and serve as “honeypots” (software designed to lure unsuspecting

people in, then compromise them and report them to law enforcement). This includes RiseUpVPN along with other services associated with them.

The Tor Browser (torproject.org) is one of the most secure available and is what is used to access the *darknet*.

4.1. Using the Tor Browser

Tor should be used only under special circumstances which require a high level of privacy. Using Tor for general (*clearnet*) internet activity will make it trivial for law enforcement to identify you. This also extends to, for instance, logging into personal accounts (for instance, on FaceBook, Twitter, YouTube, etc.) while using Tor and so on.

Tor is best used in tandem with the Tails operating system (tails.net), the details of which may be found on their website.

5. Conclusion

Transitioning away from bourgeois, privacy-invasive software at all levels is needed for any communist

movement in the Digital Age. If we follow these suggestions relevant to operations security in tandem with a proper security culture, any attempt by the capitalist state to attack our organization or our individual members. will be made many times more difficult if not impossible.

Workers of the world, unite!