Surveillance Self Defense Collective
Surveillance Self Defense #1
Things to Consider About VPNs
2/21/2025

usa.anarchistlibraries.net

Surveillance Self Defense #1

Things to Consider About VPNs

Surveillance Self Defense Collective

2/21/2025

Contents

things we have not covered here, or is not as stringent as our description. Ultimately, it is your decision which risks are acceptable, and which risks aren't. There are as many different threat models as there are people or organizations, and they can change based on what one does, says, or whom one associates with. Tools that may be acceptable for one threat model, may be insufficient for others. It is important to think about what can happen, what is likely to happen, and what one can do to mitigate those risks. Perhaps in a future article, we can talk about threat modeling and what that process looks like.

Stay safe, stay anonymous, stay active,
Surveillance Self Defense Collective

tant to keep in mind that even relatively privacy "friendly" states can still be hostile upon request of another government. Cooperation of international, national, district, and local law enforcement agencies is on the rise. For the political dissident, it is important to keep this in mind. If your country of residence is hostile to political speech that falls outside of the "norm" (hint, that's most of them) then choosing another state with higher privacy standards may be helpful… up to a point. If you are engaged in certain kinds of direct action, do not make the mistake of assuming this will protect you.

Physical location of the infrastructure (read: computers) involved in the VPN; such as the server, or servers you are routing your traffic through; is another thing to consider. Servers in countries that are hostile to political speech in general should be avoided, and should be assumed to be compromised. Servers in countries that are hostile to your particular kind of political speech may also be wise to avoid. When available, bouncing your connection between multiple different VPN endpoints may be useful, as it increases the effort required to trace those connections. Some CVPN apps offer this kind of functionality. Note that layering two different CVPN services to "double VPN" likely does little to help you stay anonymous, depending on the circumstances. It is usually better to use a single service that allows multiple "hops", and if you are concerned enough to be considering this, perhaps a technology such as TOR would better solve this need.

But I don't like any of the options

If, during this discussion, you have decided that none of the CVPNs available on the market meet your needs, you are not alone. Anonymity projects, such as TOR, may be substituted or layered to improve privacy. Before you do this, however, you should do the necessary research to determine whether *any* solution fits your needs and threat model. It may be that your threat model includes

What is a VPN?

A VPN, or Virtual Private Network, technically speaking, is a private network of computers connected over an encrypted protocol. Depending on how it is implemented, computers may talk to each other, the VPN server, and even networks outside of the VPN by routing traffic over an encrypted connection. There are several different types of VPNs, based on their technical protocol implemented, and each protocol has it's own security and privacy implications. Not all VPNs are alike, especially when talking about commercial VPN services, hereafter referred to as CVPNs to differentiate them from the protocol. VPN protocols come in a few different forms, from the popular ones such as OpenVPN and Wireguard, to other, more obscure or older protocols such as IPSec. Other anonymity projects, such as TOR, FreeNet, and I2P are outside the scope of this article, but may be mentioned for comparison.

The implications of how secure or private a VPN is depends entirely on how it is implemented. VPNs, by their nature, use a client/server model in most implementations. This means that one computer, the server, acts as the authority hosting the connection, while other computers, the clients, connect to the server. Clients can be privileged or unprivileged, but by default, the server maintains control of the connection and routes all the traffic. This inherently makes the server the weakest link in the chain, and capable of de-anonymizing you.

What is Privacy and Security?

Privacy and security are fundamentally different things. Privacy in the context of a VPN or other network obfuscation can be defined as the difficulty in attributing any particular traffic to any particular computer or user. High privacy implementations attempt to obfuscate user traffic in such a way that no traffic can be

tied to a particular computer or network. Security, however, refers to something else entirely. It speaks to the capability of an attacker to subvert or disrupt Confidentiality, Integrity, or Availability of data. The CIA triad refers to the ideas of security theory. Confidentiality is the principle of whether or not the data in question is confidential to unauthorized users. In other words, can Alice talk to Bob in a way that Eve can not understand. Integrity refers to whether or not the data has been tampered with. In other words, can Eve change the data Alice sent to Bob, with or without understanding what that data is, or what it changed to. Availability refers to whether or not the data is available to authorized users. In other words, if Alice cannot ensure Bob has access to the message she sent, that would be a low security model. You can have security without having privacy, but it is very difficult to have privacy without security.

Threat Model

A threat model is an idea in information security that refers to a portfolio of risk. Depending on your political activity, you might include many or few things in your threat model. In this step, it is important to be thorough, as it will inform all the choices you make regarding your security and privacy. In the context of radical politics, it's important to think about any potential consequences of your actions and words. Do you face potential criminal liability? How severe is it? What potential agencies might be involved in enforcement? What kind of budget do they have to bring to bare? The threat model of an insider to an intelligence agency is not the same as the threat model of someone involved in the destruction of private property. What about social consequences? What about civil consequences? We suggest you spend a decent bit of time on this analysis, really ferreting out the answers to as many questions as you can think to ask that might influence risk.

Hide in the Crowd

Next, I will talk about number of users. The way that a CVPN anonymizes your traffic is by taking the traffic of many users, and making it appear as though it originates from the same place. A good CVPN has many servers, in many different countries, with many different users connected to each of them. While this is great for general web browsing, assume that every time you log into a website with personal information, such as an email, a password, a phone number, a cookie, a token, etc. you have been identified and the traffic you created before is one step closer to being tied to your identity. Each breadcrumb you leave is a potential thread for a savvy attacker to pull. Using a CVPN is as much about operational security as it is about the technology. Any time you wish to do something that may identify you, assume you should connect to a different server. There is a helpful feature of some CVPN apps called "split-tunnel", which may allow you to log into certain services, websites, or apps outside of your normal VPN traffic, helping to mitigate the risk of a sign-in being traced to your VPN endpoint. For instance, separating your social media accounts, apps, websites, or otherwise traffic from the traffic of your normal or radical web browsing.

Locations

Legal location of the business of origin's headquarters is another metric to use when determining whether a CVPN is a good fit for your threat model. US companies have to comply with US law, EU-based companies have to comply with EU regulation and the regulation of their country of origin. Choosing a company based in countries with strong privacy law can meaningfully inhibit the state of your residence from being able to subpoena information from them. However, in an increasingly global world, it is impor-

better choice, as it may be more difficult for them to log your connections, but don't count on it. Even strictly anonymity projects that can be used like a VPN such as TOR are not immune from state action. If you're curious as to why, look up timing attacks on the TOR network.

Payment Methods and other Personally Identifiable Information

Payment methods, IP addresses, and other Personally Identifiable Information are some of the primary ways in which state and federal agencies can track your CVPN connections back to you. Depending on the implementation of the CVPN's infrastructure, they may be able to trace certain connections, sessions, or traffic back to your payment method, email address, phone number, IP address, or even password that you use. While some of these methods are more anonymous than others, assume all of them can and will eventually be traced back to you unless you take precautions. Cryptocurrency, without diving too deep into the technology, is a public ledger. Any purchase of tokens made via credit card can be traced back to you eventually. When purchasing and paying in cryptocurrency, assume that each transaction can identify you. Perhaps the safest method of acquiring cryptocurrency is by trading goods or services directly for crypto with people who cannot identify you. Also, assume that any "free" as in money CVPN is selling their logs and traffic data, at best to data brokers, at worst to the state directly. Running VPN servers at scale is not cheap. Expect to pay no less than 4–5 USD/Euro a month when paying monthly for a CVPN service. Anyone who can meaningfully undercut this price point likely has other sources of income (like selling logs and DNS data). The best CVPN services allow you to pay in cash via the mail. However, also be weary of what you put on the envelope. Depending on their disposal methods and other policies, it may be possible for an insider to still identify you through this method.

Once you have this information, the next questions to ask are about probability. How likely is this scenario that I have thought up to become a reality? What is the level of motivation of the threat I have identified? How likely is this threat to notice me? It might be useful to assign a scale of numbers to this category. Make sure you choose a spread of numbers large enough to account for various levels of motivation and probability, or use a fractional scale.

Next, you assign levels of impact. How much will this affect me and those I care about if this threat becomes reality? Again, a numerical scale is helpful in this context. Be realistic. Depending on where you are, and the threats you've identified, the scale might have a different meaning. In one person's case the top of the scale might be imprisonment, in another case it could be worse.

Finally you decide, based on the threats and the numbers you have written down, whether to accept or mitigate the risk. Keep in mind that you may, in nearly every case, need to accept at least a portion of the risk, even if you mitigate it. There may not be ways to mitigate enough risk for the probability of a realized threat to be acceptable to you. If this is the case, perhaps changing your behavior is the only way to acceptably mitigate that risk.

Keep in mind that your threat model can and will change. As your actions and words change, so does your threat model. It may be that as you continue through your radical actions, that the threats you identify become more or less serious, and your needs change as a result. It's important to not become complacent and continue thinking about this. As you graduate up into higher levels of risk, so too should your mitigations change.

How do I choose a good CVPN?

A CVPN, and the level of anonymity it provides, can be chosen based on multiple factors that determine whether or not they have both good Privacy and good Security. It's important to note

that each CVPN offers different levels of anonymity based on their policies, infrastructure, where they are located, how you pay, how many average users they have, and which server you choose when connecting to a server, among other factors. Let's break this down.

Client/Server Model

Because VPN technology is based almost entirely on the client/server model, it is important to understand all CVPNs as inherently hierarchical structures. Whether any given CVPN can be useful to you depends on trust. Trust is a tricky question in the field of information security, but it essentially boils down to transparency. Is the CVPN you want to use providing you enough information to determine whether or not they are telling the truth about their implementation, and are they taking measures to ensure they cannot meaningfully comply with any government orders for information on a given user? Ultimately, you must decide whether you trust that the company is doing enough to anonymize your traffic, even in the case of a subpoena for information. Any thread in a garment is eventually connected to another thread, and it only takes one good pull on one thread for the whole garment to unravel. Such is the nature of information security.

Policies

There are some policies that a company can take to prevent being able to provide enough information to identify you based on your traffic. Here are a few to chew on.

No Logs Policy

As VPN technology is inherently hierarchical, the biggest threat is compromise of the server by a malicious actor. This can be a malicious hacker, government agent, or even an employee for the company you're paying! VPN servers, by their nature, allow logging of many different connection details. Some VPN technologies, such as Wireguard, make compromises that can harm privacy as a trade off for speed. A Wireguard VPN server, by design, keeps the IP addresses of all connected peers in the server's working memory. An IP address is as good as a physical address to a government agent, as they can look up what Internet Service Provider owns that netblock, and subpoena that company for the records on who connected to that IP from X time to Y time. Your ISP will *always* fold to a court or sometimes even law enforcement order, legal or not; they are not your friend in staying anonymous. Likewise it is safe to assume that most if not all CVPN providers will happily give any information they have on you over to a court or law enforcement agency. There may even be money changing hands. Do not assume they are your friends in anonymity. A no logs policy just means that the company has less information to give to a court if they are subpoenaed.

VPN Technology Choices

Good VPN technology choices in respect to privacy depend on your threat model. It is important, when choosing a CVPN, that you define your threat model. As this is explicitly written for political dissidents, we're going to assume your threat model includes such organizations as Federal or State intelligence agencies. While it may be nigh impossible to properly defend yourself against such an agency using a CVPN if they're willing and able to cooperate with foreign intelligence or law enforcement agencies, you can significantly improve your anonymity and make it more difficult to identify you. Wireguard, in the case of cooperation of multiple law enforcement agencies, may not be a good choice for anonymity as any agency powerful enough to compromise the VPN server and watch it's memory can make their own logs. OpenVPN may be a