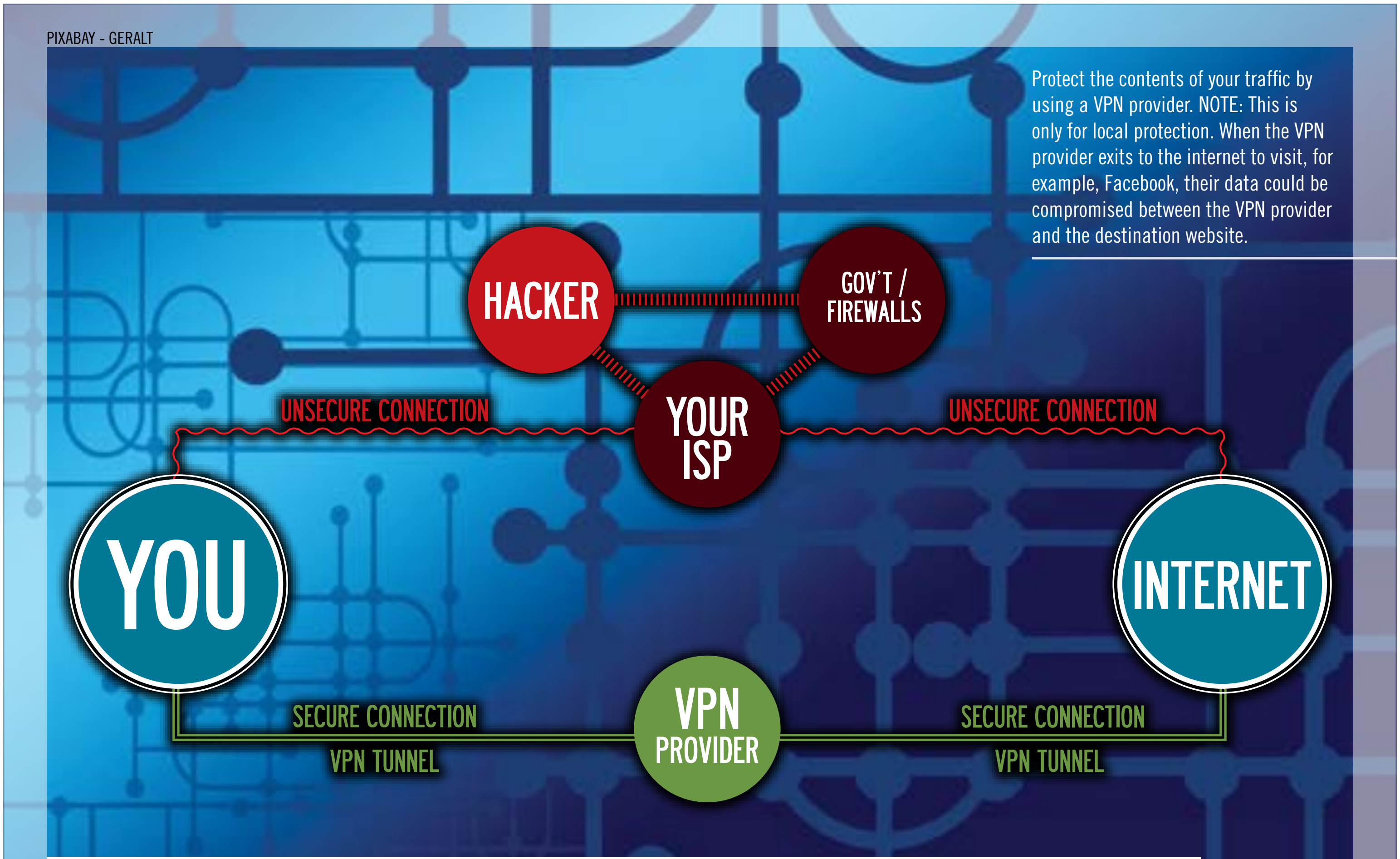
PIXABAY - GERALT



Protect the contents of your traffic by using a VPN provider. NOTE: This is only for local protection. When the VPN provider exits to the internet to visit, for example, Facebook, their data could be compromised between the VPN provider and the destination website.

DIGITAL PRIVACY TOOLS

We live in a time where nearly the entire human base of knowledge is freely available online—often times from a device we carry with us in our back pocket.

BY: DR. BRANDEN R. WILLIAMS

Any time we access this great source of knowledge, order a pizza or shop online, we leave digital fingerprints and breadcrumbs all over the Internet. Of course, the destination site will contain some of these breadcrumbs that identify your session, but you also leave fingerprints on every single router, switch or firewall that services your session.

Some of the details of our online activity can be masked through encryption technologies, tradecraft (burner phones, tablets and laptops) and operational security. Yet, researchers constantly impress us with better capabilities of tracking down individual internet users through real-time analysis of traffic at key choke points, de-cloaking attacks that subvert some of the operational security techniques we use and solid data analysis of an ever-increasing data set of internet usage.

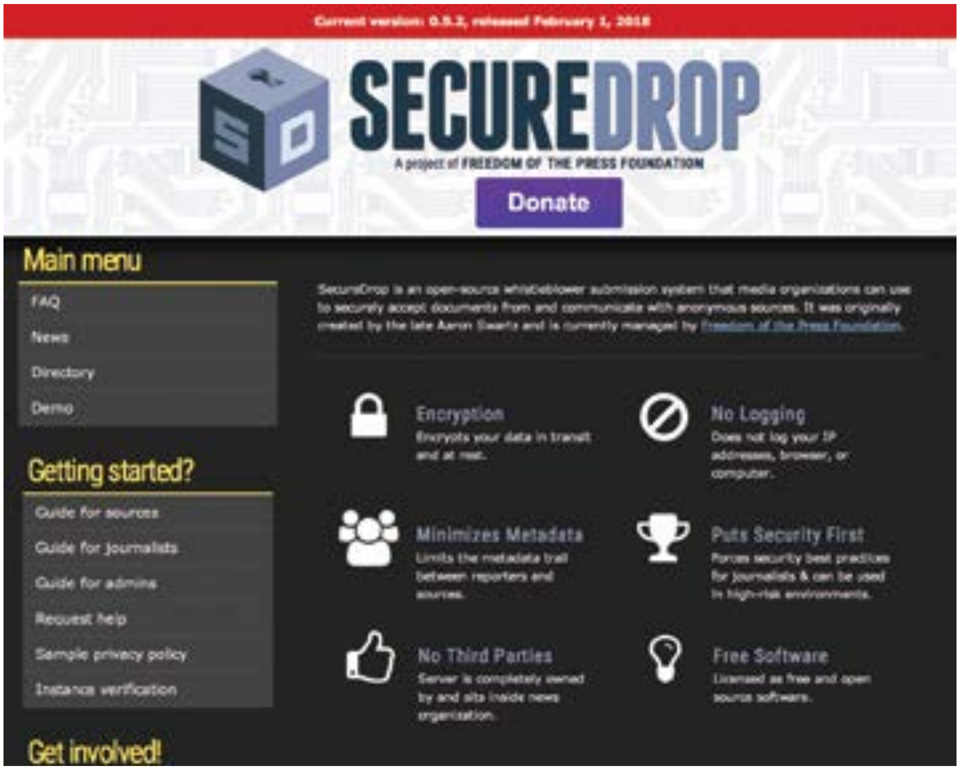
Is there anything that can be done to privately access the Internet? As it turns out, there are some tools freely available that can improve your privacy.

A STATE OF CONSTANT MONITORING

Dr. Edmond Locard, often referred to as the Sherlock Holmes of France and credited with developing major advancements in forensic science, formulated a basic premise that underpins our ability to investigate crime: every contact leaves a trace. The Locard Exchange Principle says that a criminal will both bring something to a crime scene (such as DNA) and take something with them (such as dirt or fibers), exchanging matter or properties while committing an act. What's interesting is this principle also applies in the digital world and can be used to track and monitor you.

Companies track our online behavior for advertising purposes and researchers are publishing ways to get around basic anonymization techniques that tech savvy Internet users deploy. Essentially, the keys to real privacy in the digital world rely on the security of the message exchanged, hiding the true origin and/or destination of the message and ensuring you can hide or mask the protected message well enough so patterns cannot be discovered and it disappears into the background noise.

The Internet was designed to be open and resilient. The goal being that a military strike at one node wouldn't tear the entire network down. When you look at the traditional three major pillars of information security (confidentiality, integrity and availability), the designers of the Internet largely ignored the first, at a high level ignored the second, and embraced the third.



Current version: 0.5.2, released February 1, 2018

SecureDrop is an open-source whistleblower submission system that media organizations can use to securely accept documents from and communicate with anonymous sources. It was originally created by the late Aaron Swartz and is currently managed by Freedom of the Press Foundation.

Encryption
Encrypts your data in transit and at rest.

No Logging
Does not log your IP addresses, browser, or computer.

Minimizes Metadata
Limits the metadata trail between reporters and sources.

Puts Security First
Forces security best practices for journalists & can be used in high-risk environments.

No Third Parties
Server is completely owned by and sits inside news organization.

Free Software
Licensed as free and open source software.

SITES LIKE SECUREDROP ARE USED TO SAFELY SEND FILES, OFTEN USED BY WHISTLEBLOWERS OR PEOPLE IN COUNTRIES WITH STRONG NETWORK MONITORING LIKE CHINA.

Because of the distributed nature of the network, every bit of data that comes from your phone or computer travels over multiple devices that connect you to the destination. If you want to see this in action, open up a command prompt on your computer and type this command without the quotes, “tracert 8.8.8.8”. If you are on a Mac, open your terminal and type “traceroute 8.8.8.8”. What will come back is a list of all the routers that your packets touched on the way to this public name server. Any of those routers can see the data inside your packets, which is why encryption is so important to protect the confidentiality of data.

But encryption is not enough. Because certain kinds of traffic look exactly the same every time, such as logging in and out of your email account, researchers have figured out ways to infer the contents of certain kinds of traffic even if they cannot directly observe it. Things like the destination address and how much data is transmitted can clue someone in to what the contents of those packets might be.

TWO ITEMS TO KEEP SAFE

In order to become anonymous (or pseudo-anonymous) online, you must focus on protecting two things: you must protect the contents of your traffic as well as identifying features of the two endpoints. In some cases, you can do both at the same time. As an example, you can subscribe to a service called a Virtual Private Network (VPN) from providers all over the internet.

What this does is create a secure tunnel between you and the provider, and all of your internet traffic must go through that tunnel first, so anyone around you (for example, at an open Wi-Fi Hotspot) won’t be able to see the contents of your traffic, but they can tell you are connected to a VPN service provider. Depending on what data you are passing, observers may be able to determine things you are doing such as checking email, searching on Google or browsing product pages on Amazon.com.

VPN technology is in use everywhere, allowing companies to leverage the cheaper public Internet to connect workers and locations as opposed to expensive direct high-speed lines. It provides a baseline set of security, irrespective of the security capabilities of the clients and servers used inside the tunnel. As an example, a VPN tunnel that leverages Internet Protocol Security (IPSec) would protect an insecure connection to an unencrypted web application in the same network.

THE ONION ROUTER

In order to provide another option for hiding traffic and providing anonymous services that are very difficult to trace, a group of researchers from the U.S. Naval Research Laboratory created The Onion Router or Tor for short (information at www.torproject.org). Tor is made up of groups of nodes, and after connecting to the Tor network, your connection is routed to several nodes before hitting an exit node out to the internet. Thankfully, our friends at Tor recently made accessing Tor and onion sites much easier by releasing the Tor Browser. It’s effectively a custom implementation of the popular Firefox browser, but that also means that security bugs in Firefox can sometimes be found in the TOR browser.

If you want to try Tor out, the easiest way is to download the Tor Browser from the URL above. Once you install and open the program, you can go to any website and see how you are being routed. For example, I loaded up my website after opening the Tor Browser and my connection was routed through Germany, then France, then Liberia before exiting out to the internet.

The IP address shown in the screenshot (https://www.dropbox.com/s/hf28hdl-do7nrbpu/Screenshot%202018-02-20%20 14.03.49.png?dl=0) matched what I pulled from my logs. My home IP address did not appear, and the true source of the traffic was concealed from my server. You can also try the Tor Messenger product, which is designed to leverage Tor to send secure and anonymous messages between two individuals.

TOR VULNERABILITIES

Anyone can run a Tor node, which should make you start to ask questions. *Could a government run one?* Yes, and many vocal Internet privacy supporters suspect that several agencies already do this to target opponents that leverage the Internet to run. In fact, a popular use case of Tor is providing darkweb marketplaces and information bureaus that can only be accessed via Tor. There are both legitimate (privacy and security) and illegitimate (selling or trading illicit items) reasons to do this.

Trusting Onion sites can be a challenge. For example, it is completely reasonable that the FBI could conduct a sting operation via an Onion site to catch criminals selling or trading illicit goods and services. If you envision SilkRoad reborn, the site could offer simple things like selling narcotics to more complex things like purchasing the services of a hitman.

The U.S. government also interfaces with Tor to track down criminals who run these successful hidden Onion sites. The FBI's Operation Torpedo in 2011 compromised Onion sites so they would push specially modified code down to users, revealing their true IP address. This technique is called decloaking, and it resulted in a number of raids and arrests of Tor users.

Tor has gotten much more secure over the years as evidenced by the surprisingly large number of vulnerabilities discovered and fixed in the platform. It's great for creating casual anonymity, but it may not protect you fully against a sophisticated adversary. As always, understanding the technology you are using and having some kind of confirmation on the authenticity of the content you are accessing via Tor is critical to your safety.

PRACTICAL TOOLS FOR PRIVACY

Edward Snowden revealed both a number of tools and techniques used by the NSA to collect intelligence as well as showed how technologies such as Tor can be used to get around this monitoring. There are, of course, completely legitimate reasons to securely exchange information between parties—a digital dead drop. Here is a list of additional tools that you might find useful:

TAILS (https://tails.boum.org) is an operating system that aims to preserve privacy and anonymity. You follow the instructions to put it on a USB stick and then boot a computer/laptop from that USB stick for a completely anonymous and temporary computing experience. This would be useful if you are using someone else's computer to access sensitive documents, and do not want to leave any traces on their computer.

Signal Messenger (https://signal.org) is a secure messaging platform that allows for messages to disappear over time. This is useful if you want to send short "text" messages with confidential instructions or messages (such as financial data) that do not stay resident on devices. Keep in mind, however, that once the message reaches the other side, that person may put your identifying information in screen shots.

SecureDrop (https://securedrop.org) is a secure way to exchange files between parties. It is most commonly used by sources who want to blow the whistle on governments or corporations by anonymously sending documents to journalists. It could also be used to exchange files securely in countries with strong network monitoring such as China.

Ad blockers are a useful extension to add into your browser to stop advertising tracking of online behavior. If you use and deploy one, you will stop receiving ads for products you search for inserted into your typical online browsing. Check your browser's plugin store for one that may work well for you.

ADDITIONAL READING

For more information how three math visionaries solved an incredibly complex problem to provide the framework for confidentiality on the internet, check out this simplified Wikipedia article on the RSA Algorithm: http://brando.ws/RSAAlg

For a fantastic write up on how TOR can be less anonymous, read this Vice article: http://brando.ws/vicetor

Looking for a VPN service? Check out this list of providers by PCMag: http://brando.ws/2017-vpn ✓

BIO

Branden R. Williams, DBA, CISSP, CISM (www.brandenwilliams.com) is a seasoned security executive, ISSA Distinguished Fellow, and technology executive sought by global companies to consult on their digital business initiatives. His latest book on PCI DSS v3.2 Compliance is available on Amazon.

GEARREVIEW

X-22 HUNTER STOCK

The X-22 takedown chassis is specifically designed for the Ruger 10/22 Takedown series of rifles. It is reinforced polymer, with adjustable length of pull and comb height to fit a wide variety of shooters and fit in a backpack. It features multiple sling mounting options, a non-slip rubber butt-pad, and M-LOK slots for accessory attachment with no gunsmithing required. **www.magpul.com**