Society for Computers & Law
The leading educational charity
for the tech law community
www.scl.org

SCL tea and tech: demystifying the dark web by Neil Brown and Alex Bloor

Neil began by saying that the notion of the "Dark Web" conjures up images of a mythical place full of criminals and undesirables. This is scaremongering - his law firm has a presence there with its website and blog. It is a routing system and there is nothing intrinsically dark about it.

Most people attending the SCL Zoom call had not tried to access it. It was originally devised by the US Navy in the mid-1990s but eventually because a not-for-profit business in 2006 using open source.

Many organisations have services available in Tor for non-nefarious reasons. Tor stands for "the onion router" - it is so-called as it is multi-layered. The layers are encrypted and peeled off as information passes through the system. Its key aim is to protect data in transmission.

The system works through a series of nodes – a guard node, relay nodes and exit node. Tor creates a route between your computer and the computer you want to talk to. It connects you to the guard node which in turn uses relay nodes and an exit node takes you into the website. Each node strips off a lawyer of encryption and then the reverse happens on the way back to you. None of the nodes know the full path of the data and the route taken through the network can change.

People can use private gateways into Tor to avoid interference from ISPs or repressive regimes. Some ISPs have more intrusive surveillance and block traffic; "pluggable transport" stops this, although Neil said in 18 years of using Tor he's never had this problem.

Using Tor, cookies are only valid for one session. You can either route traffic through it or access sites available within it.

The Tor browser can be used like any other browser, but you can see the route the data takes. A website will see the IP address of the exit node but won't be able to see the IP address of your device. It can also be used as a proxy.

However, it protects data – it cannot guarantee anonymity.

Within Tor, websites often use captchas to make sure you are not a robot – it can be the case that you get caught in a cycle of this and never actually get to see the website you want.

So why would you want to use Tor? As an example, you may be a web developer and want to see what a website or page looks like outside your network, or how it can be accessed from outside the network.

You can avoid algorithms and price discrimination based on cookies or IP address. However, you might find that if you are accessing a website via Tor you won't be able to purchase but you can at least see the difference in price.

You may not want people to be able to see what you are accessing – for example, a law firm might not want people to know they are investigating them, or someone living under a repressive regime may not want to access LGTB websites on the open web.

Websites within Tor end with .onion. Facebook, the BBC and the CIA all have .onion websites, as does Pornhub, as it is harder to block websites in Tor.

Applied uses of Tor include onionshare, which allows you to share large (and small) files easily. Cwtch is a messaging service and Nat traversal avoids problems with not having separate IP addresses for each device you have on your network if you want people to be able to access information on a device and not interfere with your router.

There are various questions at the end of the session including topics like Tor versus a VPN; does Tor use more energy with all its routing; and a question about whether there is a search engine, there isn't, you need to know the web address or use a curated list of websites. The most recent versions of web addresses in Tor are very long and created using cryptography.