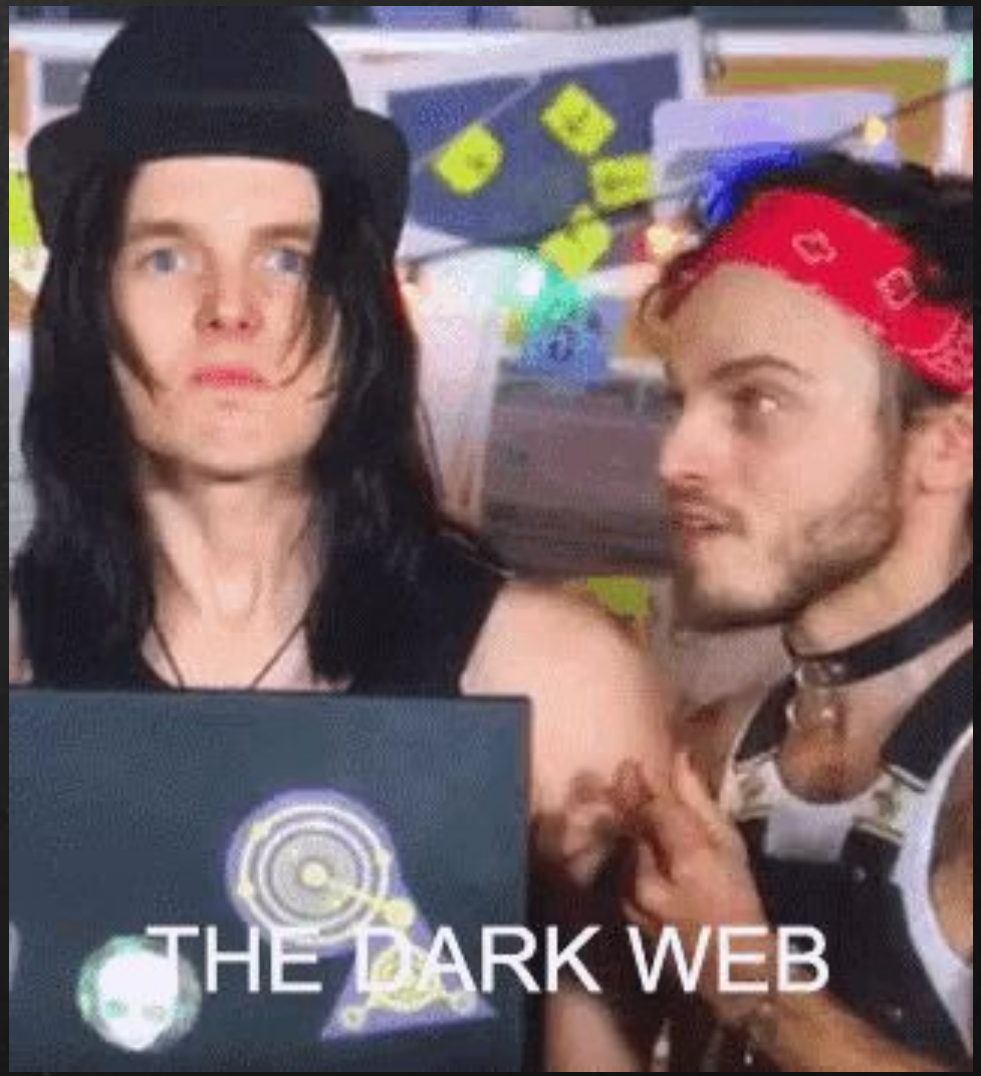
A Gentle Introduction To the DARK WEB!!!

OLUG
April 07, 2026

By Aaron Grothe

Welcome to The Dark Web!!!



Introduction

If you have questions/comments please feel free to ask them anytime. You don't have to hold them until the end of the talk.

If there are other resources similar to these that you think might be useful to people please let the group know.

I'm still learning this stuff out and I might know the answer :-(

Hopefully this will be an interactive and productive session.

Slides will be at https://grothe.us

Disclaimer

We are talking about the Dark Web

Bad things do happen on the Dark web (E.g. the Silk Road) and the regular web as well

If you do anything bad or illegal or anything bad or illegal happens to you on the dark web, I'm sorry

As always use your best judgement at all times

Dark Web - Survey

How many of you have used TOR?

How many of you have tried out the Dark Web?

How many of you think you know what the Dark Web is?

How many of you have used a VPN?

What is the Dark Web???

The Three Layers of the Web

- Surface Web (Clear Web): The classic "visible" internet. This is any site that search engines can search and find. This is about 5% of the internet
- Deep Web: Web not indexed by search engines. Behind security walls. Think Gmail Inbox, banking portals, private databases. Majority of internet is here
- Dark Web: Subset of the Deep Web that is intentionally hidden. Requires specific browsers, and requires using Tor, I2P, or another system to access

Intro

What we're going to cover tonight

- FAQs about Tor
- Getting onto the Tor Network
  - Firefox Tor Browser
  - Routing your internet traffic through Tor
  - Bringing NEbraskaCERT's website onto Tor
  - Next steps - Whonix, Tails, I2P, etc.
  - 6 TIps for a Better Experience
  - Conclusion

FAQs about Tor

Who made Tor?

- U.S. Naval Research Laboratory (NRL) in the mid-1990s

What was the initial purpose of Tor?

- Was made to protect US Intelligence communications

How many people use Tor?

- Estimate is it is in the millions

Primary Goal

- Anonymous access to the public Internet (Clearnet)

FAQs about Tor (Cont'd)

How does Tor work?

- Onion routing. Your data is wrapped in multiple layers of encryption. It then passes through three volunteer nodes (Entry, Middle, and Exit).
- At the Exit node the data leaves the Tor network and hits the Clearnet to talk to a regular website E.g. Wikipedia, google.com, etc. Or it can go to an .onion site :-)
- The response flows back to the exit node which layers it again and sends it back through the net to the user

FAQs about Tor (Cont'd)

How Secure is Tor?

- Quite simply it is about as good as it gets. There are issues if you can own an exit and entry node you can do traffic correlation to get a good idea about who the traffic is from
- HTTPS helps prevent eavesdropping, owning just an entry or exit node only lets you know the middle relay node's IP address
- There have been timing attacks and other issues against the Tor Network, but these have been patched pretty quickly

FAQs about Tor (Cont'd)

How Secure is Tor?

- Tor does not prevent an application from sharing your IP address. E.g. WebRTC and Bittorrent both will reveal your IP address
- Tor does not support UDP traffic
- There are potential issues with DNS lookups over TCP with some older implementations

Getting Onto the Tor Network

We'll start with the Tor Browser

- Hit the tor project - https://torproject.org
- Download the Tor browser
- Download the Tor browser signature
- Cd to download directory
  - $ cd Downloads

Getting Onto the Tor Network

We'll start with the Tor Browser

- Validate the tor browser
  - Grab the key - "gpg --auto-key-locate nodefault,wkd --locate-keys torbrowser@torproject.org"
  - Verify the key gpg --verify \
    tor-browser-linux-x86_64-xx.x.x.tar.xz.asc \
    tor-browser-linux-x86_64-xx.x.x.tar.xz
  - If it doesn't say good signature, delete it

Getting Onto the Tor Network

Extract the browser

- Cd back to home directory
  - $ cd ~
- Extract the tarball
  - $ tar xvf Downloads/tor-browser-linux*gz
- Cd to the tor-browser directory
  - $ cd ~/tor-browser
- Start the browser
  - $ ./start-tor-browser.desktop

First Test - What is my IP?

We'll use two browsers for this test - regular Firefox and Tor browser

Verify IP addresses

https://ipchicken.com

If these match, we're in trouble :-(

Second Test - How Fast is this?

Comparing internet speed of regular Firefox and Tor Browser

Checkout Internet Speeds

https://speedof.me

Tor is slower, or should be.

Second Test - Why is Tor Slower?

Two main reasons?

- We're routing our traffic through 3 nodes
- We're encrypting it multiple items and stripping the encryption off

You're trading speed for safety

Hit an Onion Site.

So far we're just using the Tor browser to securely hit Clearnet sites

Lets hit the https://tornews.com/deep-web/lists/dark-web-sites/ - to find a good site.

We'll hit ProtonMail

https://protonmailrmez3lotccipshtkleegetolb73fuirgj7r4o4vfu7ozyd.onion/

So you can sign up for an email account without handing out personal info

Data Leakage

We'll hit https://coveryourtracks.eff.org and compare the amount of data leaked by regular Firefox and the Firefox Tor browser

Regular Firefox: 18.25 bits of identifying information
Tor Browser: 10.6 bits of identifying information

More importantly other Tor browsers have the same fingerprint as we do. The regular ESR browser is UNIQUE

Quick Notes - Need to Repeat

Tor by default only routes TCP traffic, not UDP

So bittorrent and a lot of other file sharing and gaming things are not well suited for the Tor network.

You can install Tor and NFtables on your box and have it route all TCP traffic through the Tor network. There are issues with DNS and any UDP services that might leak your address. Recommend the Tor Project browser, or a custom Linux version like Tails or Whonix

Bringing NEbraskaCERT onto Tor

For this we're going to talk about how we brought the NEbraskaCERT website onto the Dark Web :-)

- https://www.nebraskacert.org is the official website of NEbraskaCERT
- NEbraskaCERT is a local Computer Security group that has a lot of content people might like to hit

The webserver runs on Debian 13/Trixie and uses Apache/Httpd as the webserver

Steps to Getting on Tor Network - Part 1

Need to install Tor on the box

- $ sudo apt-get -f install tor

Setup basic tor

- $ sudo vi /etc/tor/torrc
- Uncomment the following lines
  - HiddenServiceDir /var/lib/tor/hidden_service
  - HiddenServicePort 80 127.0.0.1:80

Note: We're using port 80 as 443 is encrypted and we'll have issues with the certificate, we're only listening on the local port so not an issue

Steps to Getting on Tor Network - Part 2

Restart tor to generate the private key for this

- $ sudo systemctl restart tor

Get your hostname

- $ sudo cat/var/lib/tor/hidden_service/hostname

This will restart tor and generate a hostname and public and private key for the website

Steps to Getting on Tor Network - Part 3

Need to setup the webserver to make website available via tor

- $ cat /etc/apache2/sites-available/onion.conf

```
<VirtualHost 127.0.0.1:80>
#    ServerName
joqlq2qaf2t7no5fhgu562v6bwd4zxwbfizcy3b3ioxrz2nmthilbbid.onion
   DocumentRoot "/var/www/html/www.nebraskacert.org"

   # Security: Disable logs or anonymize them
   ErrorLog ${APACHE_LOG_DIR}/onion_error.log
   CustomLog ${APACHE_LOG_DIR}/onion_access.log combined

   # Optional: Prevent the server from revealing its real IP in headers
   ServerSignature Off
</VirtualHost>
```

Steps to Getting on Tor Network - Part 4

Verify the config

- $ sudo apache2ctl configtest

If this comes back clean time to restart the webserver

- $ sudo systemctl restart apache2

Fire up the Tor browser and go to the website

http://necertwg77m7hhxcruw7547hibhzzhdfbodemzz2g47a24klw6cv2mad.onion/

Steps to Getting on Tor Network - Part 5

Getting a Vanity Address

You can use mkp224o to generate an onion address that is closer to your domain name

$ ./mkp224o -n 1 necert -d final

Notes: You're having a program generate lots of keys for you. The longer you make it the longer it takes. necert only takes a minute on my aipc, nebraskacert would take a lot longer

Tips - 6 Tips for a Better Experience

1. Start with either the Tor Browser or Tails on a USB stick
2. Tails on a write protectable USB stick is a good thing
3. Be patient, you're going to pay an overhead for using Tor
4. Tor is a great way to do research on topics you're concerned about
5. You'll learn a lot in the process, don't be scared to experiment
6. If you're going to do a Tor website, a foreign VPS is a good idea

Next Steps - Part 1

Things I didn't talk about tonight but are related

- Ghost Laptops - these are laptops that are designed to be harder to track. Buy anonymously, remove camera, speakers, microphone, wifi etc.
- I2P - Invisible Internet Project - is a more decentralized system compared to Tor, not as popular but very interesting in some ways superior
- Whonix is interesting it can creates two machines either real or virtual and you force all traffic on it to go through tor
- Whonix on QubesOS is very interesting
- Buying a cheap Mango Pi router and set it up to do Tor and have it be a Tor middlebox

Next Steps - Part 2

Things I didn't talk about tonight but are related

- Whonix is interesting it can creates two machines either real or virtual and you force all traffic on it to go through tor
- Whonix on QubesOS is very interesting
- Buying a cheap Mango Pi router and set it up to do Tor and have it be a Tor middlebox
- Mullvad browser is a version of Firefox that incorporates most of the Tor improvements but is designed to be used with a VPN
- Onionshare - very cool file sharing app

Tor Pro/Cons

Pros

- Censorship resistant
- Unmatched Anonymity
- Pretty easy to setup and use

Cons

- Dangerous content (potentially illegal)
- Security vulnerabilities
- Expectation of Privacy
- People doing bad things on the Tor network

Summary

This is a very gentle/quick introduction to the Darkweb

I believe the net benefits of Tor far exceeds the negative use of Tor

Setting up a Tor website, will teach you some new things

Thanks

Thanks for Listening

Any Questions?

Links

Tor Project

- https://www.torproject.org/

Cover Your Tracks from EFF

- coveryourtracks.eff.org

Links

Ghost Laptops - Nice Youtube video

- https://www.youtube.com/watch?v=EHW2XseuDDo

Ghost Laptops - a Short presentation

- https://www.grothe.us/presentations/techtalkers-202602-ghostlaptops.pdf

Links

Tails Linux Distribution

- https://www.tails.net/

Invisible Internet Project (I2P)

- https://i2p.net/

Whonix - Very Cool In-depth Security Linux Distribution

- https://www.qubes-os.org/

Links

Qubes OS

- https://www.qubes-os.org/

GL.inet - Mango Pi Router

- https://store-us.gl-inet.com/

Mullvad Browser

- https://mullvad.net/en/browser

Links

OnionShare

- https://onionshare.org/

NEbraskaCERT website (Normal)

- https://www.nebraskacert.org

NEbraskaCERT website (Tor)

- http://necertwg77m7hhxcruw7547hibhzzhdfbodemzz2g47a24klw6cv2mad.onion/