# A Gentle Introduction to the Dark Web

NEbraskaCERT | August 19, 2026

Presenter: Aaron Grothe

# WELCOME & GUIDELINES

## Interactive Session

Feel free to ask questions anytime. No need to wait for the end of the presentation.

## Participation

Please share similar resources you find useful. This is a learning experience for everyone.

## Slides Available

Access these materials at grothe.us or via the NebraskaCERT site.

# LIABILITY & GUIDANCE

*"The Dark Web is where both good and bad things occur, just like the regular web."*

**I am not responsible for illegal activities or anything that happens to you. Use your best judgment at all times.**

# DEFINING THE INTERNET

## Surface Web

Visible and indexed. Searchable by Google/Bing. ~5% of the total internet.

## Deep Web

Not indexed. Behind logins (Banking, Private DBs). The vast majority of the web.

## Dark Web

Hidden subset requiring specific software like Tor or I2P to access.

# PRESENTATION AGENDA

- FAQs: Origins and Goals
- Getting onto the Tor Network
- Verifying the Tor Browser
- Routing traffic through Tor
- NEbraskaCERT on the Dark Web
- Next Steps (Whonix, Tails, I2P)
- Tips for a better experience
- Pros/Cons and Conclusion

# ORIGINS AND SCALE

### The Creators

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

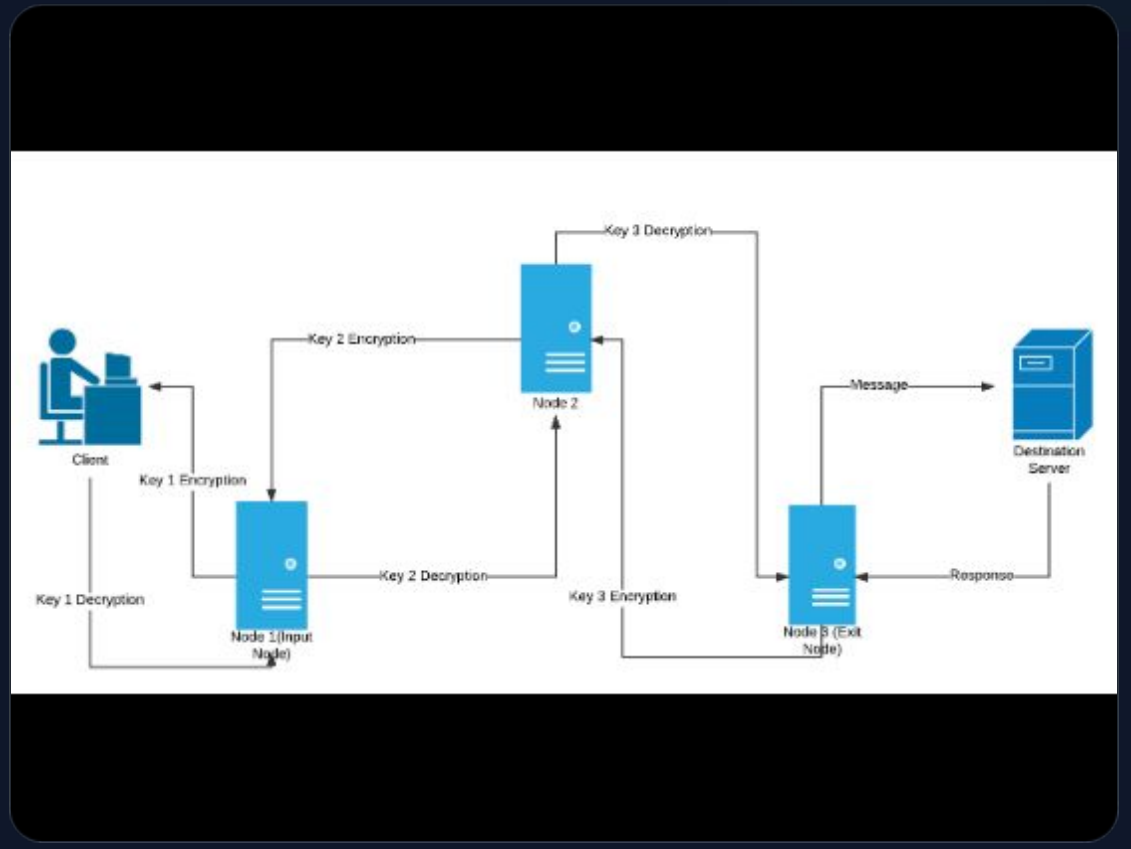
### Primary Purpose

Protecting U.S. Intelligence communications from external analysis.

Today, millions of users utilize Tor for anonymous clearnet access.

# ONION ROUTING LOGIC

- **Layers:** Data is wrapped in multiple layers of encryption.
- **Nodes:** Traffic hops through Entry, Middle, and Exit relays.
- **Exit:** At the exit node, data hits the Clearnet or a .onion site.



# SECURITY STATUS (1)

### Resilience

Generally as good as it gets for current anonymity technology.

### Correlation

Risks exist primarily if one entity owns both the entry and exit nodes.

### HTTPS Integration

Mandatory for preventing exit node eavesdropping of plaintext data.

# SECURITY STATUS (2)

- **IP Exposure:** Tor does not stop apps from leaking your IP (e.g., WebRTC).
- **Protocol Limits:** Tor does not natively support UDP traffic.
- **DNS Leaks:** Potential issues exist with older TCP-based DNS implementations.
- **Timing Attacks:** Vulnerabilities are patched quickly by the community.

# INITIAL SETUP STEPS

**Download**

Get the bundle from torproject.org

**Signatures**

Download the browser signature file

**Verify**

Validate the integrity of the binary

# CRYPTOGRAPHIC VERIFICATION

1. Import Key:

```
gpg --auto-key-locate nodefault,wkd --locate-keys torbrowser@torproject.org
```

2. Verify Binary:

```
gpg --verify tor-browser-linux.tar.xz.asc tor-browser-linux.tar.xz
```

> If signature is NOT "good", delete the file immediately.

# EXTRACTION AND EXECUTION

**Unpack**

tar xvf Downloads/tor-browser*gz

**Start**

cd ~/tor-browser
./start-tor-browser.desktop

# TESTING ANONYMITY

IP

**Verify your public identity**

Use **ipchicken.com** in both standard Firefox and Tor Browser.

**If IP addresses match, you have a configuration leak!**

# TESTING ANONYMITY 2

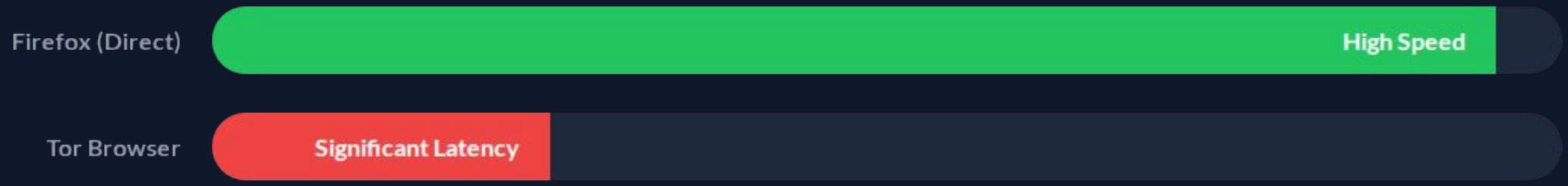

## Verify you are on the Tor network

Visit **check.torproject.org** using your Tor Browser.

**If the page says you are NOT using Tor, stop immediately!**

Your connection is exposed and your real IP is visible.

# TESTING PERFORMANCE




Expect performance hits when testing with **speedof.me**.

# THE LATENCY TRADE-OFF

- **Encapsulation:** Multiple layers of encryption take time to process.
- **Routing:** Traffic travels through three distinct physical nodes.
- **Geography:** Nodes are often located on different continents.
- **Bottom Line:** You are sacrificing speed for safety and anonymity.

# HITTING .ONION SITES

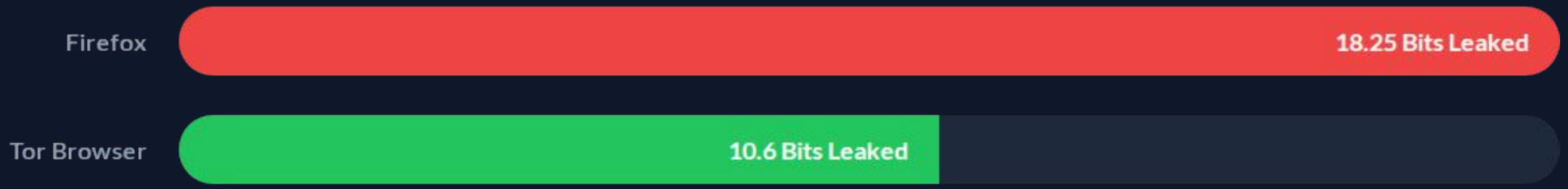
**Moving beyond Clearnet**

Example: ProtonMail (.onion)

```
protonmailrmez3lotccipshtkleegetolb73fuirgj7r4o4vfu7ozyd.onion
```

Onion services allow users to interact with platforms without disclosing personal metadata.

# BROWSER FINGERPRINTING




Verification tool: **coveryourtracks.eff.org**

# TRAFFIC REALITIES

## TCP Only

Tor routes TCP by default. UDP is not natively supported.

## Poor Fit

BitTorrent and online gaming are not well-suited for Tor.

## Preference

Use Tor Browser, Tails, or Whonix instead of manual configurations.

# NEbraskaCERT on Tor

A Guide to Dark Web Hosting

# HOSTING SETUP (1)

- **Install:** sudo apt-get -f install tor
- **Configure:** Edit /etc/tor/torrc
- **Settings:** Enable HiddenServiceDir and HiddenServicePort 80

# HOSTING SETUP (2)

### Activation

sudo systemctl restart tor

### Host Identity

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

This command reveals your site's permanent .onion address.

# WEB CONFIGURATION

- **Virtual Host:** Configure Apache to listen for the onion address.
- **Hardening:** Set ServerSignature Off to hide versioning.
- **Privacy:** Disable or anonymize logs in the Apache config.

# TESTING THE SERVICE

### Config Check

apache2ctl configtest

### Restart

systemctl restart apache2

### Access

Browse the .onion URL

# VANITY ADDRESSES

**Customization**

Use tools like **mkp224o** to generate addresses with specific starting characters.

> Trade-off: Longer custom prefixes take exponential computing power to generate.

# TIPS FOR A BETTER EXPERIENCE

- Start with Tor Browser or Tails.
- Tails on write-protected USB is recommended.
- Be patient (significant overhead).
- Great for deep research.
- Don't fear experimentation.
- Consider foreign VPS for hosting.
- Some sites (e.g. olug.org) block Tor.
- Used by orgs like MI6.
- Can set exit node country in torrc.

# ADVANCED RESEARCH

### Ghost Laptops

Hardened laptops with physically removed peripherals.

### I2P

Invisible Internet Project: Peer-to-peer alternative network.

### Whonix / Qubes

Advanced multi-machine isolation for network traffic.

# PRIVACY TOOLS

## Mullvad Browser

Firefox-based, VPN-oriented focused browser.

## OnionShare

Open-source tool for anonymous file sharing and chat.

# THE BALANCE SHEET

## Pros

Censorship resistance, unmatched anonymity, and ease of deployment for sensitive research.

## Cons

Dangerous content, security vulnerabilities in legacy apps, and negative public reputation.

# KEY TAKEAWAYS

- The Dark Web is a misunderstood tool for privacy.
- Net benefits of the tech far exceed the negatives.
- Hosting your own service is a premier learning opportunity.

# Questions?

Thank you for your attention.

**Aaron Grothe** | NEbraskaCERT

grothe.us | nebraskacert.org

# Resources & Links

Reference Material for Further Study

# CORE PRIVACY LINKS

**Tor Project:** torproject.org

**Cover Your Tracks (EFF):** coveryourtracks.eff.org

**Tails Linux:** tails.net

**Privacy Guides:** privacyguides.org/en/

# ADVANCED OS & I2P

- Qubes OS / Whonix: qubes-os.org
- Invisible Internet Project (I2P): i2p.net

# HARDWARE & TOOLS

- **Mullvad Browser:** mullvad.net/en/browser
- **OnionShare:** onionshare.org
- **GL.inet Mango Pi:** store-us.gl-inet.com

# GHOST LAPTOPS DEEP DIVE


**YouTube Video:** Watch Video

**Short Presentation:** Read PDF

Hardened systems for extreme field security.

# NEBRASKACERT LINKS

**Normal (Clearnet):**
nebraskacert.org

---

**Dark Web (Tor):**
necertwg77m7hhxcruw7547hibhzzhdfbodemzz2g47a24klw6cv2mad.onion