Ethical Student Hackers

Anonymisation using TOR

The Legal Bit

- The skills taught in these sessions allow identification and exploitation of security vulnerabilities in systems. We strive to give you a place to practice legally, and can point you to other places to practice. These skills should not be used on systems where you do not have explicit permission from the owner of the system. It is VERY easy to end up in breach of relevant laws, and we can accept no responsibility for anything you do with the skills learnt here.

- If we have reason to believe that you are utilising these skills against systems where you are not authorised you will be banned from our events, and if necessary the relevant authorities will be alerted.

- Remember, if you have any doubts as to if something is legal or authorised, just don't do it until you are able to confirm you are allowed to.

- Relevant UK Law: https://www.legislation.gov.uk/ukpga/1990/18/contents

Code of Conduct

- Before proceeding past this point you must read and agree to our Code of Conduct - this is a requirement from the University for us to operate as a society.
- If you have any doubts or need anything clarified, please ask a member of the committee.
- Breaching the Code of Conduct = immediate ejection and further consequences.
- Code of Conduct can be found at **shefesh.com/conduct**

Anonymity

Encryption is not anonymous, it is just the process of scrambling data so outsiders can't view what you're communicating

When you use things like incognito mode, websites can still track your IP Address and other information about your browser

Anonymity means your data is **hidden** and **untraceable** when browsing the internet

Browser Anonymity

Every Browser has a **‘fingerprint’**

This is a list of characteristics unique to a user, their browser, and their hardware setup

This fingerprint consists of:

- Installed fonts
- Screen resolution
- Time Zone
- Device platform
- And many more

Browser Anonymity

https://coveryourtracks.eff.org/

https://clickclickclick.click

HASH OF CANVAS FINGERPRINT

c99af7d79a238cf2e0d6037f143046ca

One in *x* browsers have this value: *263.49*

ARE COOKIES ENABLED?

Yes

One in *x* browsers have this value: *1.06*

Your Results

Your browser fingerprint **appears to be unique** among the 285,356 tested in the past 45 days.

Currently, we estimate that your browser has a fingerprint that conveys **at least 18.12 bits of identifying information.**

What is TOR?

TOR stands for **T**he **O**nion **R**outer

Onion Routing is a technique which relies on routing your internet traffic through many different volunteer operated nodes (routers)

The TOR protocol uses 3 ‘hops’ across nodes in the TOR network to provide anonymity

Essentially acts like a proxy server

3-Node System

TOR encrypts your data 3 times - creating 3 layers of encryption

Entry Node (Guard Node) - Removes first layer of encryption, sees address of middle node and forwards data

Middle Relay (Relay Node) - Removes second layer of encryption, sees address of exit node and forwards data

Exit Node - Removes final layer of encryption and reveals actual request (“**https**://www.google.com/”)

IMPORTANT Each node only knows the previous and the next step, you can’t just retrace all the way back to the sender from the exit node

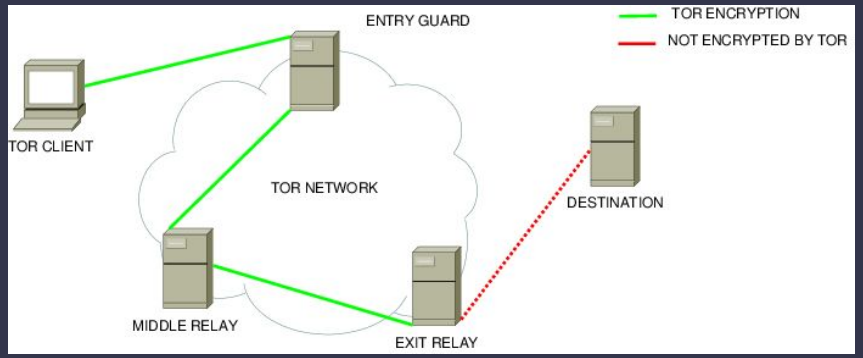
Why does it work?

There are thousands of TOR Clients using the network simultaneously, there isn't just 1 client

Conversations between nodes are designed to look like any message (first, second or last)

The path between nodes constantly changes (every 10 minutes), so tracking over time is useless

No logs are kept on TOR nodes so once the data moves forward, the past is forgotten



TOR Uses

There are many reasons why you'd want to remain anonymous whilst accessing certain parts of the web

- Conducting OSINT
- Accessing the .onion domain (Only available if you're using TOR)
- Preventing tracking
- Cryptocurrency transactions
- Whistleblowing

TOR Practical

1. Use to connect to a surface website (like sheffield.ac.uk)

2. Go to the previous websites and see what has changed

    a. https://coveryourtracks.eff.org/
    b. https://clickclickclick.click

Connect to a Tor hidden services website and see what is different

a. https://www.bbcnewsd73hkzno2ini43t4gblxvycyac5aw4gnv7t2rccijh7745uqd.onion
b. https://www.facebookwkhpilnemxj7asaniu7vnjjbiltxjqhye3mhbshg7kx5tfyd.onion
c. http://xp44cagis447k3lpb4wwhcqukix6cgqokbuys24vmxmbzmaq2qjvc2yd.onion
d. https://duckduckgogg42xjoc72x3sjasowoarfbgcmvfimaftt6twagswzczad.onion

Dark Web vs Deep Web

Deep Web - section of the internet that cannot be indexed by web crawlers
Majority of Deep Web consists of regular websites that require accounts to access

- Internet Banking
- Email inbox
- Medical documents

Dark Web - a subsection of the Deep Web that includes websites that can only be accessed through purpose-built web browsers
Main application is to provide anonymity to website owners and visitors

Problems with TOR

It doesn’t prevent man-in-the-middle attacks

TOR is illegal in some countries

Doesn’t provide complete anonymity - entering personal details can still give you away

Not all websites are available on TOR

Spyware/keyloggers on your device can still see what you are searching

TOR network hosts illegal services

TAILS OS

The Amnesiac Incognito Live System (TAILS)

- A security focused Linux distribution aimed at preserving privacy and anonymity against surveillance
- **Amnesiac** - Tails is loaded into system memory; all data is lost when the system is turned off
- **Incognito** - TOR as standard, encrypted emails, encrypted storage (if used)
- **Live system** - installable to a USB stick and can be ran off most computers

Upcoming Sessions

What's up next?

www.shefesh.com/sessions

Next week:

DRM

Any Questions?

www.shefesh.com

Thanks for coming!