Secure Internet Accessing

Basic anonymity concepts

- What do we want to hide?
  - sender anonymity
    - attacker cannot determine who the sender of a particular message is
  - receiver anonymity
    - attacker cannot determine who the intended receiver of a particular message is
  - unlinkability
    - attacker may determine senders and receivers but not the associations between them (attacker doesn't know who communicates with whom)
- From whom do we want to hide this?
  - external attackers
    - local eavesdropper (sniffing on a particular link (e.g., LAN))
    - global eavesdropper (observing traffic in the whole network)
  - internal attackers
    - (colluding) compromised elements of the anonymity system
  - communication partner

Basic anonymity concepts

- What do we want to hide?
  - sender anonymity
    - attacker cannot determine who the sender of a particular message is
  - receiver anonymity
    - attacker cannot determine who the intended receiver of a particular message is
  - unlinkability
    - attacker may determine senders and receivers but not the associations between them (attacker doesn't know who communicates with whom)
- From whom do we want to hide this?
  - external attackers
    - local eavesdropper (sniffing on a particular link (e.g., LAN))
    - global eavesdropper (observing traffic in the whole network)
  - internal attackers
    - (colluding) compromised elements of the anonymity system
  - communication partner

TLS

- TLS - Transport Layer Security (previously SSL - Secure Socket Layer)
- Protects communication over the Internet (e.g., clients and web pages, e-mails, etc.)
- S in HTTPS (HTTP don't provide security)
- Actual version is TLS 1.3 (since 2018)
- Two parts, handshake and record
- Handshake: Initialize the communication and decide security parameters
- Record: Secure data sending

TLS Handshake

1. Client connects to the server and presents a list of supported cipher suites (ciphers and hash functions).
2. From this list, the server picks a cipher and hash function that it also supports and notifies the client of the decision.
3. The server provides identification in the form of a digital certificate. The certificate contains the server name, the trusted certificate authority (CA) that vouches for the authenticity of the certificate, and the public encryption key of the server.
4. The client confirms the validity of the certificate before proceeding.
5. Generate the session key via public key cryptography.

TLS properties

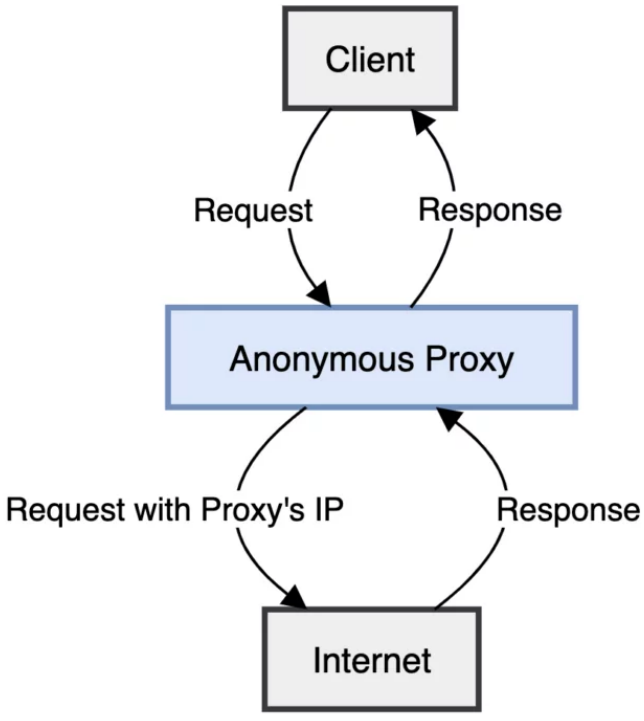
What TLS protect.

- The message.

What TLS does not protect.

- TLS does not remove information about the sender and the receiver (eavesdropper can see the identity and IP address).
- TLS does not anonymize the sender, the receiver sees the senders identity.
- TLS does not hide personal information, so the web page can collect and store them (cookies).

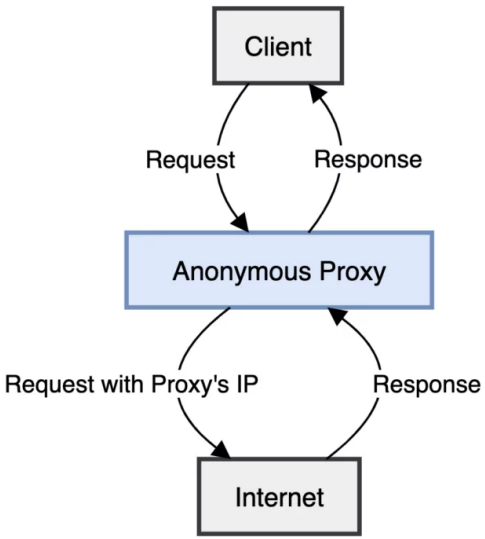
Anonymous proxy



What is an anonymous proxy?

- Application-level
  proxy that relays messages
  back and forth between
  a user and a service provider
- Ensures
  only sender anonymity with
  respect to the communicating
  partner (service provider does
  not know who the real user is)

Anonymous proxy applications



Privacy:
removes user's real IP and address

- Protect user identity
- Avoid targeted content

Access inaccessible content:
server receives the IP of the proxy

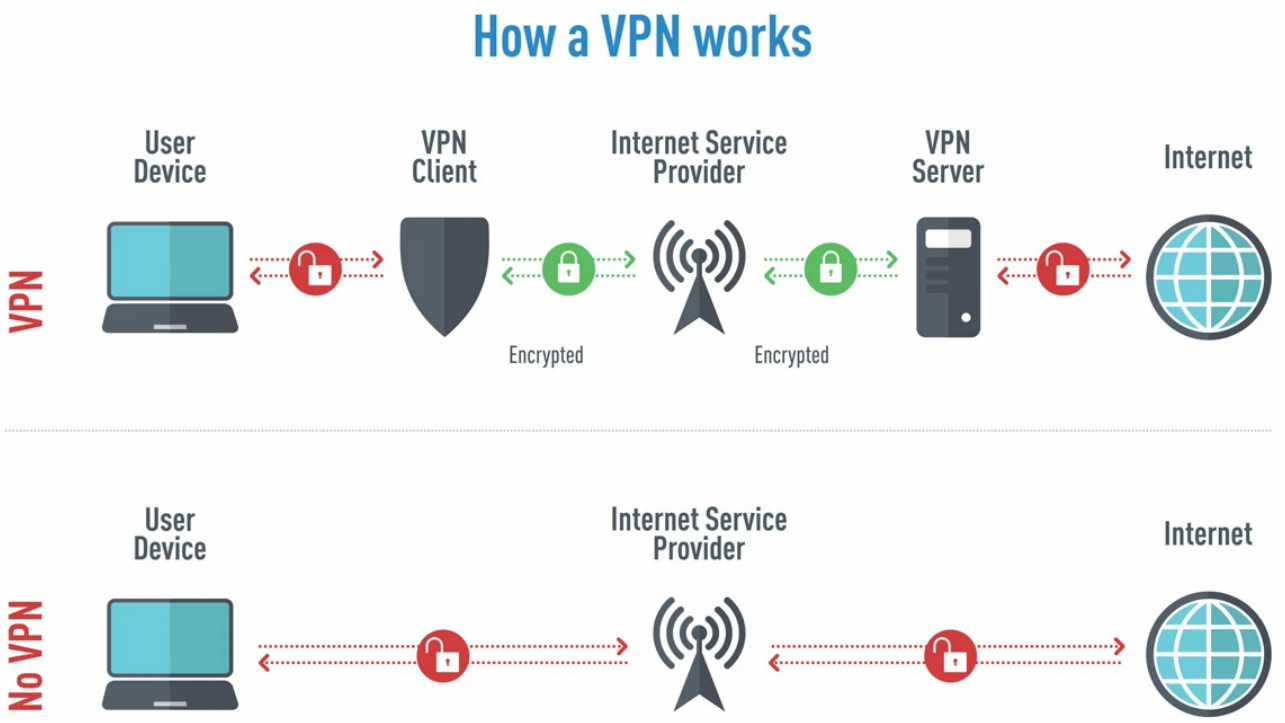
- Avoid censorship:
- Access home content

Drawbacks of anonymous proxies

- **Performance issues:** Network compatibility issues may occur between your network and the proxy provider that can cause errors.
- **Limited effectiveness:** Hides your IP, but don't use encryption to protect your data.
- **Reliability concerns:** May be slow and provide unstable connections. Some web services can also block the proxies.
- **Security concerns:** If it is hacked, your sensitive online traffic could be compromised. Malicious actors can infect your computer with malware, which would turn your computer into a proxy and possibly make you liable for its misuse.
- **Legal and ethical considerations:** The use of anonymous proxy servers is banned in some countries, such as China and North Korea.

VPN

- Virtual Private Network
- Reroutes your internet traffic through a remote server and hides your IP address.
- It works on the operating system level.
- Encrypts your traffic between the internet and device.



Anonymous proxy vs. VPN

	VPN	Proxy
Encryption	Offers encryption, securing data traffic.	Doesn't offer encryption, leaving data exposed.
Scope of operation	Operates at the operating system level, securing all traffic.	Operates at the application level, securing specific apps.
Speed	Might be slower due to encryption, but top VPNs offer high speed.	Generally faster due to lack of encryption.
Cost	Usually paid with higher quality services and support.	Often free but with less reliability and security.
Reliability	More reliable with fewer connection drops.	Less reliable with frequent connection drops.
Use case	Suitable for security, privacy, remote work, and sensitive transactions.	Suitable for bypassing geo-restrictions and basic anonymization.
Customer support	Offers customer support.	Customer support is typically lacking or non-existent.
Anonymization	Changes IP address, offering more robust anonymization.	Changes IP address but offers weaker anonymization.
Data security	Better suited for protecting sensitive or financial data.	Not suitable for protecting sensitive data.
Target user	More suitable for businesses and professional use.	More suitable for casual, non-sensitive tasks.

What is Tor?

- It's Tor (not capitalized).
- The goal is to have a way to use the internet with as much privacy as possible:
  - by routing traffic through multiple servers; and
  - by encrypting it each step of the way.
- Hence the term *onion routing*.
- Tor provides anonymity, mitigating against surveillance and censorship.

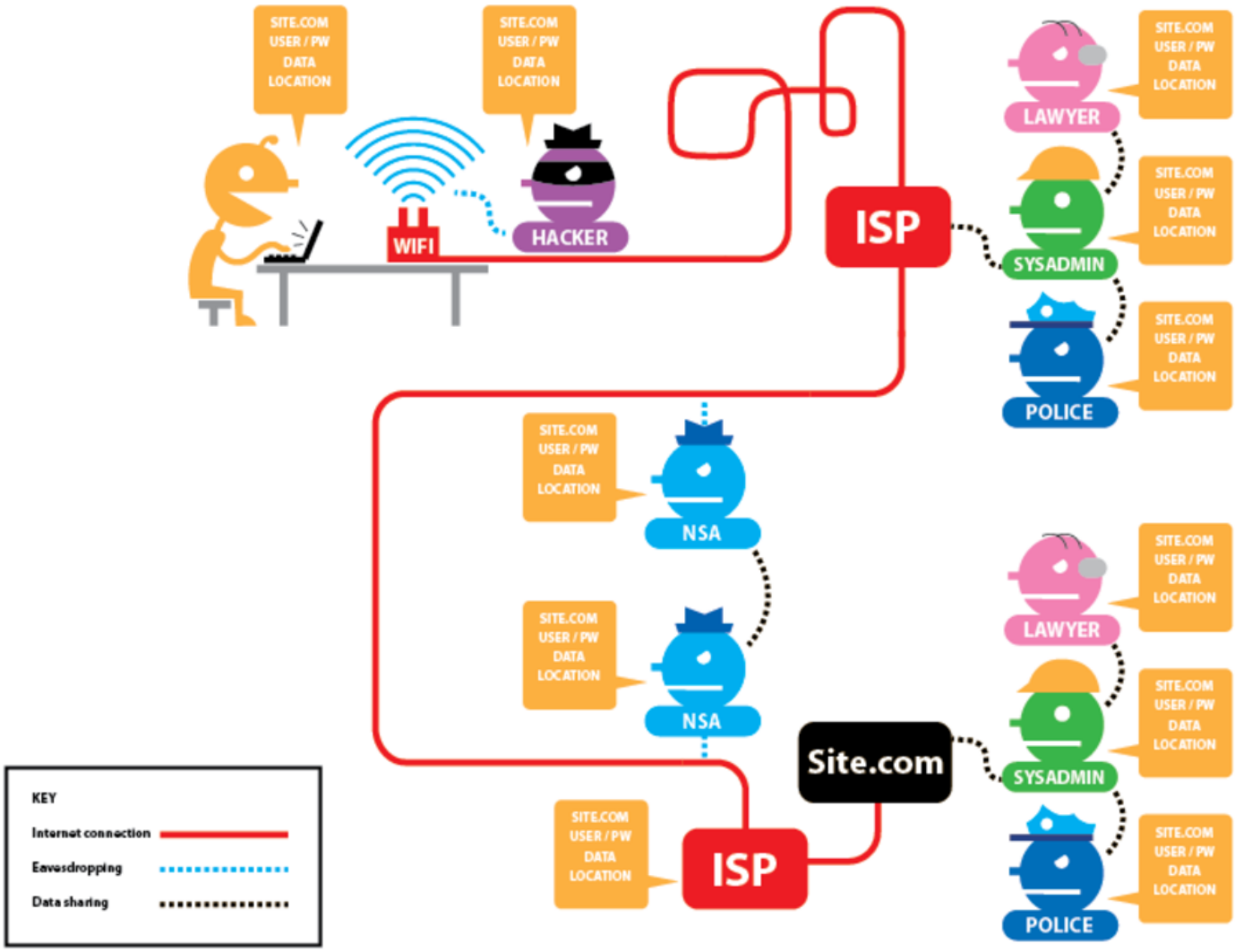
Different ways of defining Tor

- Tor $\Rightarrow$ free software created at NRL starting 2001/2.
- Tor $\Rightarrow$ an open network of 9,500 nodes – anyone can join!
- Tor$\Rightarrow$ a browser that connects you to the Tor network.
- Tor $\Rightarrow$ a US non-profit formed in 2006.
- Tor $\Rightarrow$ a community of volunteers, researchers, developers, trainers, advocates from all over the world.

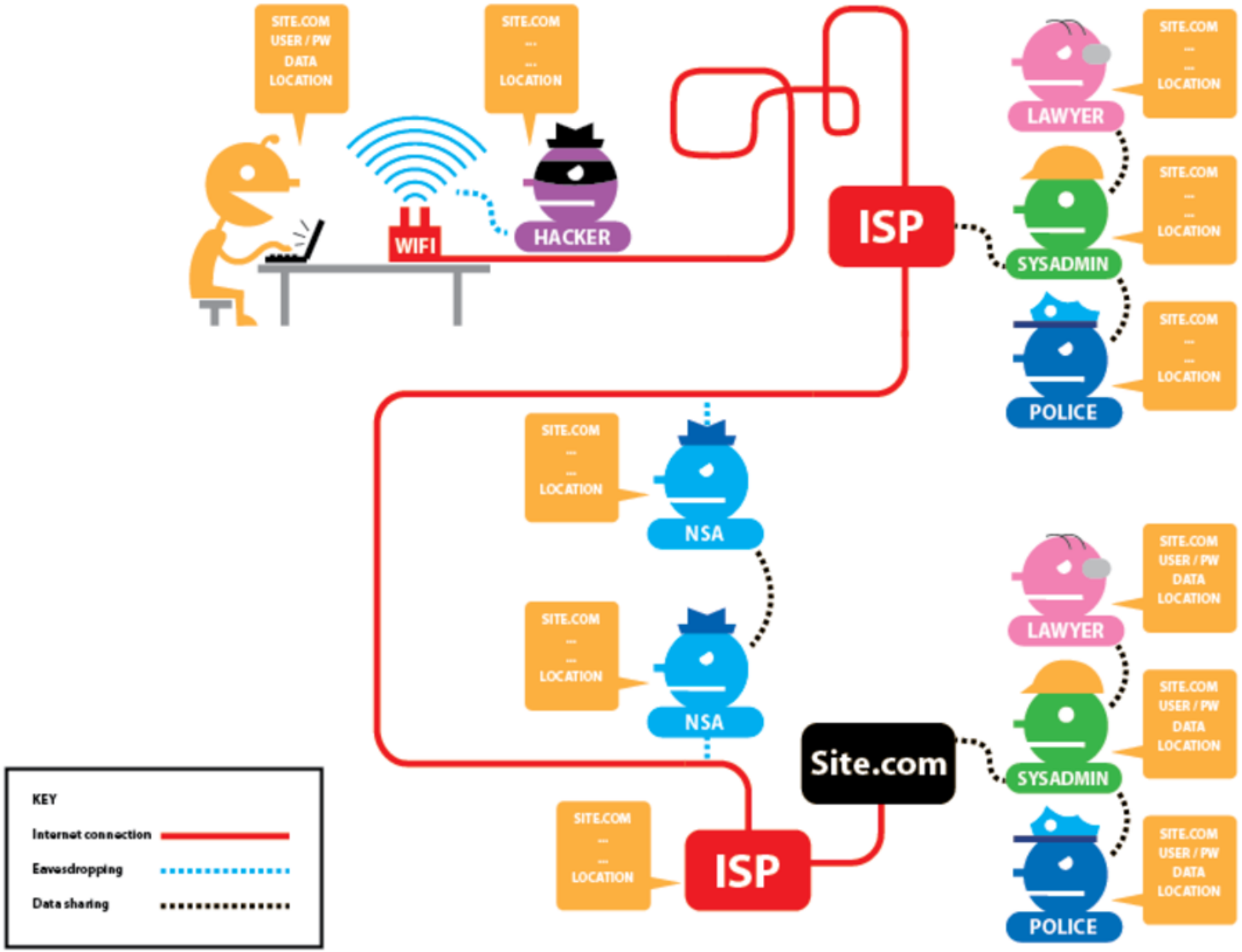
What is Tor good for?

- To resist government mass and targeted surveillance.
- To securely bypass Internet censorship.
- To counter the business model of the Internet: big data, advertising, non-consensual tracking.

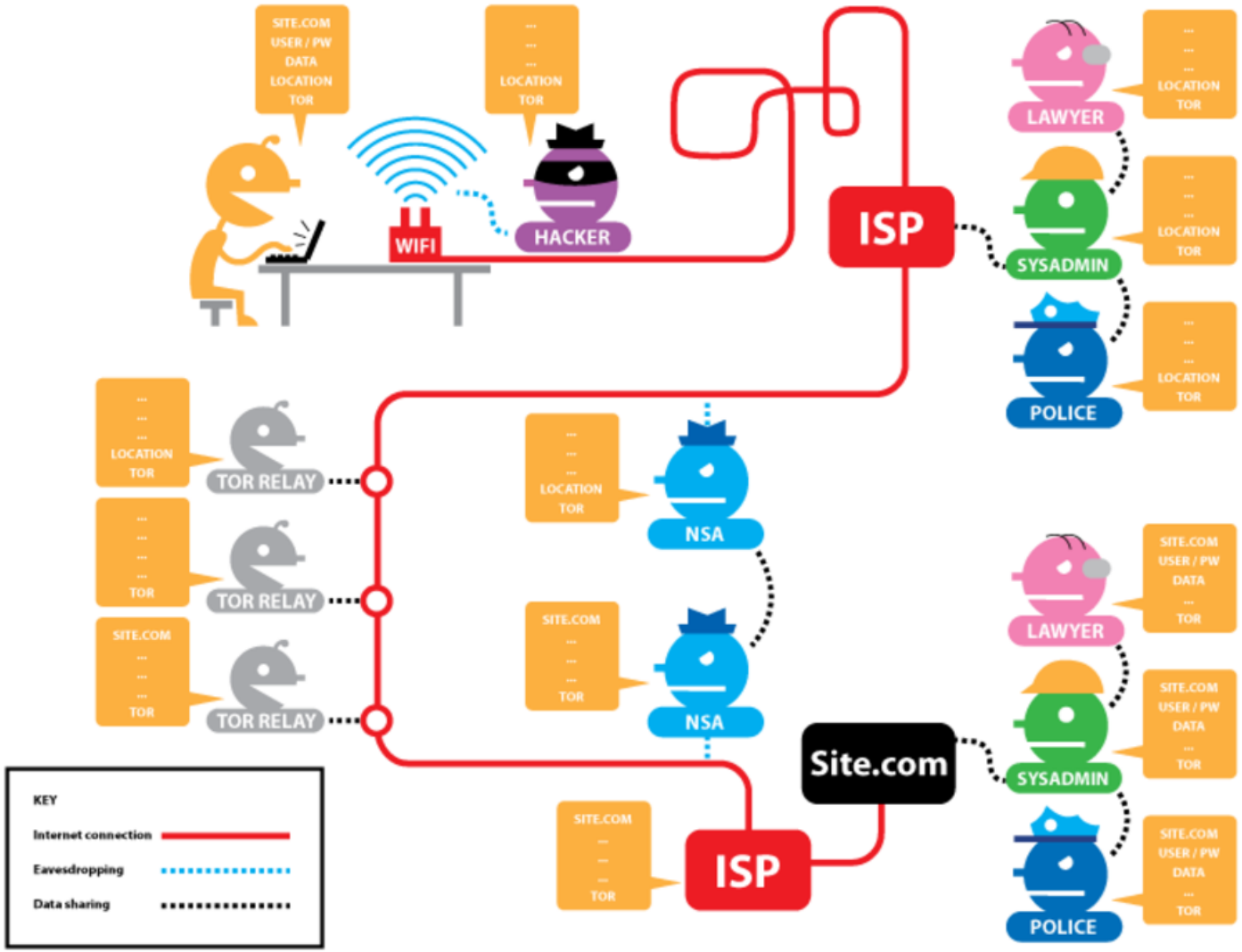
HTTP


SITE.COM
USER / PW
DATA
LOCATION
WIFI
HACKER
ISP
LAWYER
SYSADMIN
POLICE
NSA
Site.com
KEY
Internet connection
Eavesdropping
Data sharing

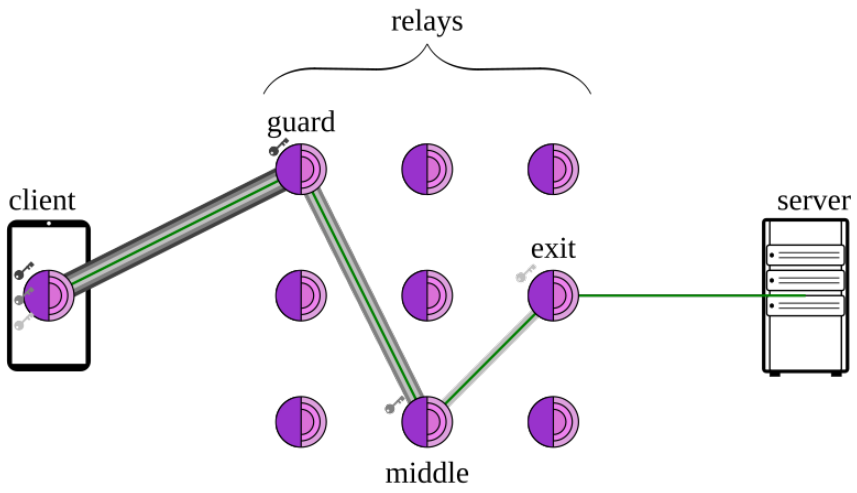
HTTPS


SITE.COM
USER / PW
DATA
LOCATION
SITE.COM
...
...
LOCATION
WIFI
HACKER
ISP
LAWYER
SYSADMIN
POLICE
NSA
NSA
Site.com
ISP
KEY
Internet connection
Eavesdropping
Data sharing

HTTPS + Tor

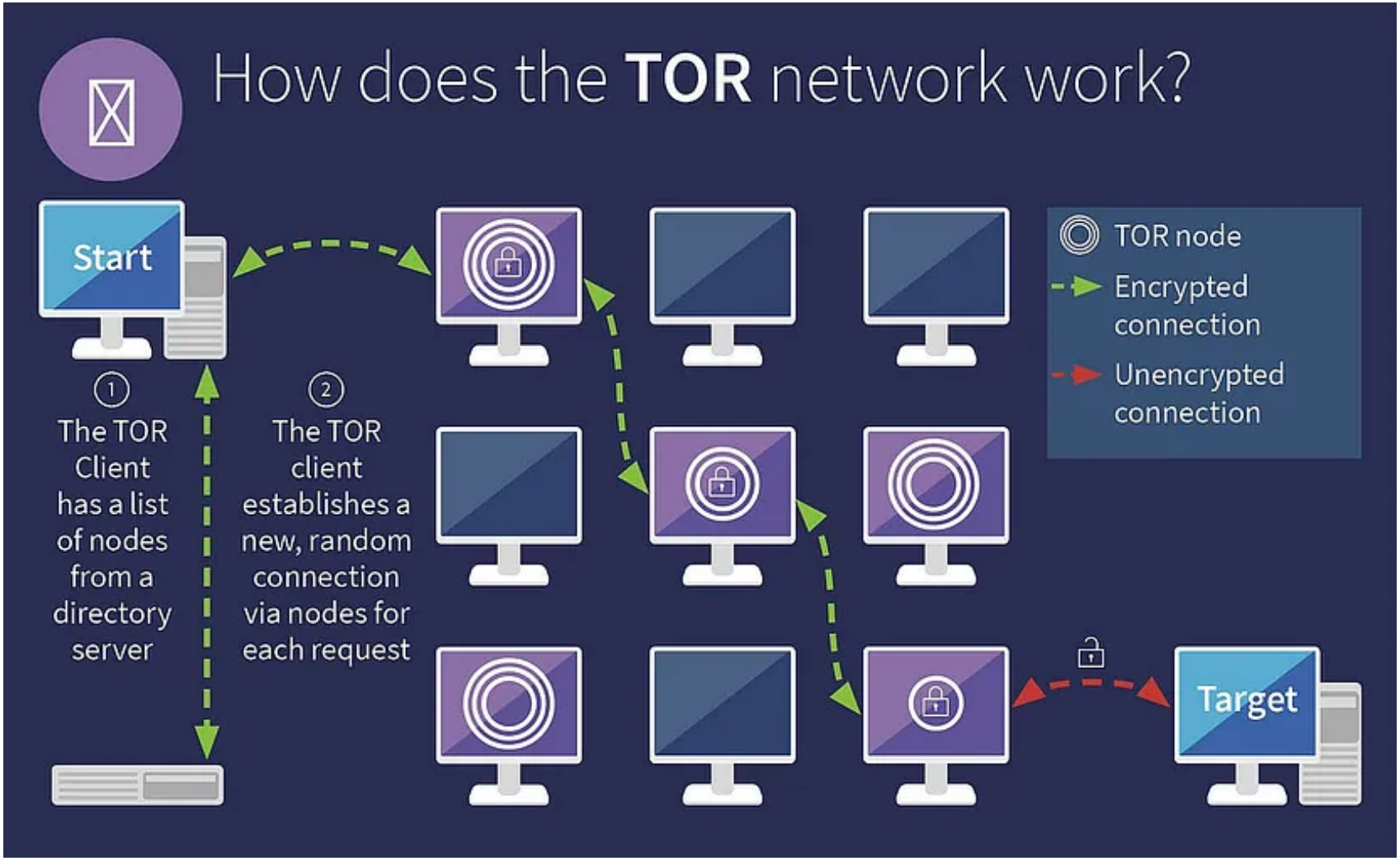

SITE.COM
USER / PW
DATA
LOCATION
TOR
LOCATION
TOR
WIFI
HACKER
ISP
LAWYER
SYSADMIN
POLICE
LOCATION
TOR
TOR RELAY
TOR RELAY
TOR RELAY
TOR
NSA
NSA
SITE.COM
TOR
Site.com
ISP
KEY
Internet connection
Eavesdropping
Data sharing

Onion routing

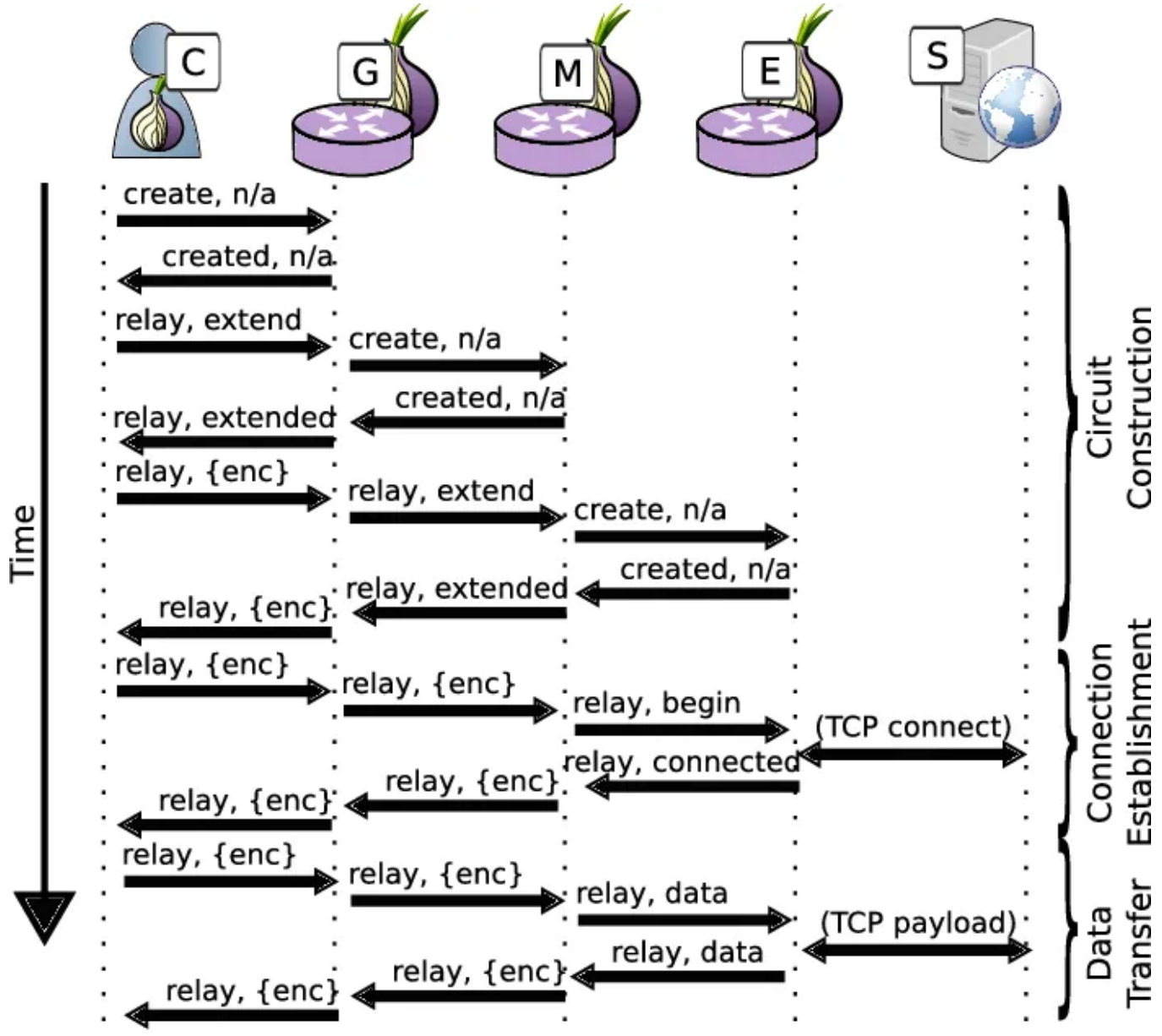


- Messages are encapsulated in layers of encryption (analogous the layers of an onion).
- Encrypted data transmitted through series of network nodes called *onion routers*
- Each peels away a single layer, revealing the data's next destination.
- After final layer: destination
- A node does not know how many nodes are in before or after it in the circuit.

Onion routing



Onion circuit



Onion creation and transmission

- Originator selects a set of nodes from a list provided by a directory node
- The chosen nodes are arranged into a path, called chain (circuit) (entry node, middle nodes, exit node)
- Originator establishes a connection and a shared secret key with every node in the list:
  - Originator establishes a connection and a shared secret key with the first node.
  - Originator establishes a connection and a shared secret key with the second node through the first node (first node relays the message).
  - Originator establishes a connection and a shared secret key with the third node through the first and second node.
- The originator encrypts the message with every session key and sends it through the nodes.
- The recipient can send a message back through the same chain. This time every node adds encryption layer to the message.

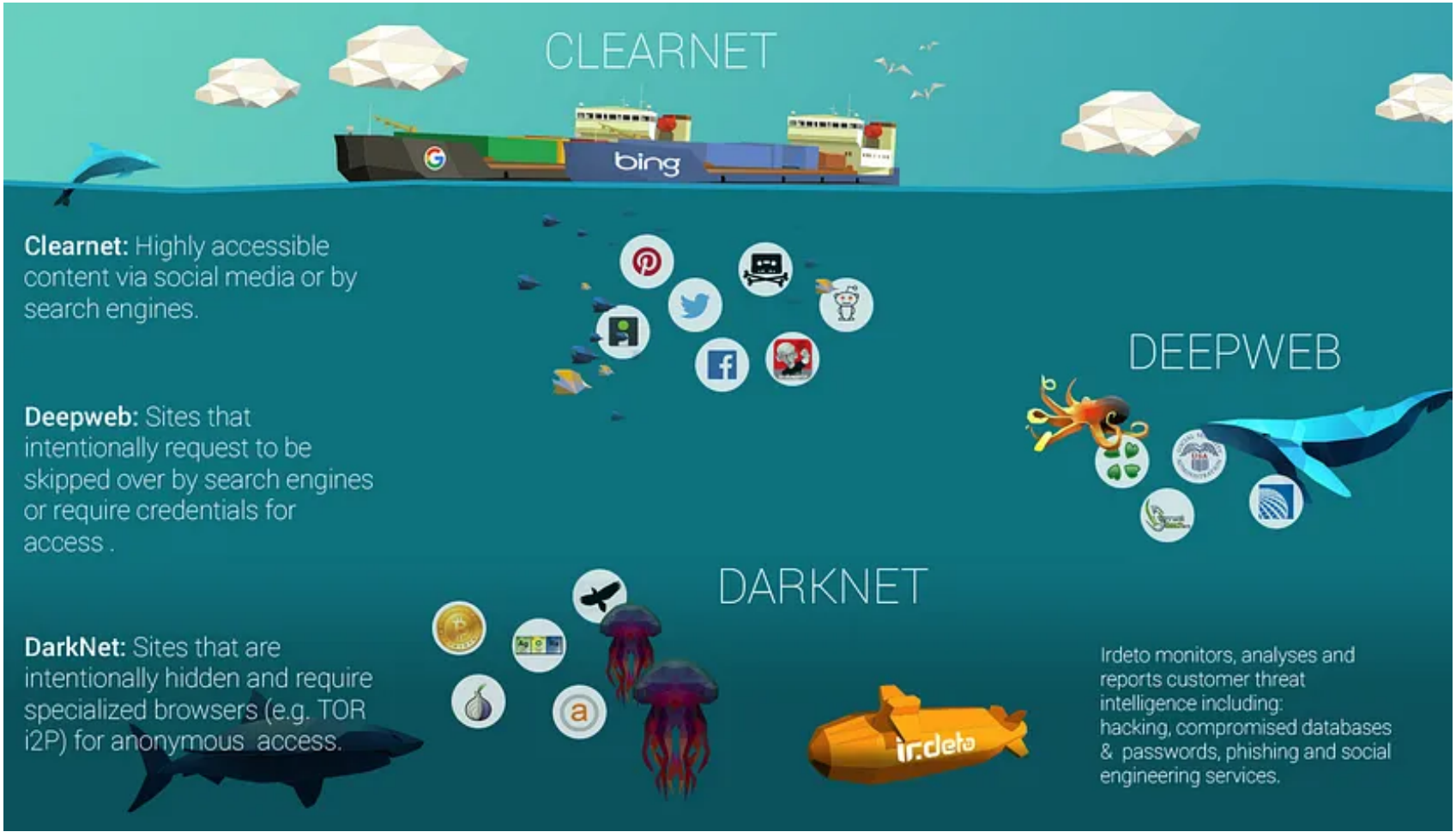
What is Tor Browser?

- Tor is a browser. You can download it from https://www.torproject.org/
- Traffic is encrypted and bounces through three random volunteer-run nodes called relays.
- Tor Browser = little-t tor + patched Firefox
- Anyone snooping can't see the websites you visit.
- Websites can't track you or see other sites you visit (cross-tracking).
- Prevents other privacy violations like fingerprinting or third-party cookies.
- Writes nearly nothing to disk.
- No browser history.
- Cross platform: Windows, macOS, Linux and Android.

Onion service

- Tor can also provide anonymity to websites and other servers
- Servers configured to receive inbound connections only through Tor are called onion services
- Rather than revealing a server's IP address (and thus its network location), an onion service is accessed through its onion address, usually via the Tor Browser
- The client and onion service each select three relays (a guard and two middle relays) to route traffic to each other, never leaving the Tor network, and never transmitting plaintext.

Onion service



Disadvantages of using Tor

- **Slow connection:** traffic goes through multiple nodes
- **Security limited only to Tor browser:** not all applications that you use on your computer can be protected by the Tor network.
- **Vulnerabilities:** Though Tor is designed for anonymity, the onion network is vulnerable at the entry and exit nodes.
- **Blocking:** Some network administrators block Tor. Some websites also keep track of and block web traffic coming from Tor exit nodes. But you can mask node usage by using Tor bridges or a VPN.
- **Stigma:** Tor has acquired the unfortunate stigma of dark web illegality. ISPs and governments may take note of people who use the browser. For people seeking privacy, Tor may bring them the opposite.