Tor

The Onion Router
Tor
Tor

- A way to use the internet ‘securely’.
Tor

- A way to use the internet ‘securely’.
- Secure meaning:
Tor

• A way to use the internet ‘securely’.

• Secure meaning:
  • Privacy
Tor

- A way to use the internet ‘securely’.
- Secure meaning:
  - Privacy
  - Anonymity
Tor

- A way to use the internet ‘securely’.
- Secure meaning:
  - Privacy
  - Anonymity
- Censorship circumvention
Most common use of Tor:
Who uses Tor?
Who uses Tor?

• Journalists

• Dissidents

• ‘Normal people’
Who uses Tor?

- Journalists
- Dissidents
- ‘Normal people’
Who uses Tor?

- Journalists
- Dissidents
- ‘Normal people’
Who uses Tor?

- Journalists
- Dissidents
- ‘Normal people’
Tor usage often correlates with political events:

Directly connecting users from Iraq

The Tor Project – https://metrics.torproject.org/
How Tor works

---

**Step 1:** Alice’s Tor client obtains a list of Tor nodes from a directory server.
How Tor works

Step 2: Alice’s Tor client picks a random path to the destination server. Green links are encrypted, red links are in the clear.
Tor circuit

- Alice knows everything
- The individual Tor nodes know (almost) nothing
- Circuit is valid for 10 minutes
- Bob is exposed
Tor Hidden Services
1. Bob creates a public key
Tor Hidden Services

1. Bob creates a public key

2. Bob creates a circuit and publishes it as his Introduction Point
1. Bob creates a public key

2. Bob creates a circuit and publishes it as his Introduction Point

3. Alice creates a circuit to a Rendezvous Point
Tor Hidden Services

1. Bob creates a public key

2. Bob creates a circuit and publishes it as his Introduction Point

3. Alice creates a circuit to a Rendezvous Point

4. Alice creates a circuit to the IP and tells Bob about the RP
Tor Hidden Services

1. Bob creates a public key

2. Bob creates a circuit and publishes it as his Introduction Point

3. Alice creates a circuit to a Rendezvous Point

4. Alice creates a circuit to the IP and tells Bob about the RP

5. Alice and Bob meet at the RP
Alice → Bob
Attacks against Tor
Attacks against Tor

- Correlation attack by:
Attacks against Tor

- Correlation attack by:
  - Being (un)lucky
Attacks against Tor

• Correlation attack by:
  • Being (un)lucky
  • Prevention by many non-adversarial nodes
Attacks against Tor

- Correlation attack by:
  - Being (un)lucky
  - Prevention by many non-adversarial nodes
- Sybil attack
Attacks against Tor

• Correlation attack by:
  • Being (un)lucky
    • Prevention by many non-adversarial nodes
  • Sybil attack
    • Prevention by directory authorities
Attacks against Tor
Attacks against Tor

- Censorship, e.g. in China, Iran and Kazakhstan
Attacks against Tor

- Censorship, e.g. in China, Iran and Kazakhstan
  - Circumvention by bridges
Attacks against Tor

- Censorship, e.g. in China, Iran and Kazakhstan
  - Circumvention by bridges
    - Private bridges
Attacks against Tor

• Censorship, e.g. in China, Iran and Kazakhstan
  • Circumvention by bridges
    • Private bridges
    • Meek bridges (Google, Amazon, Microsoft)
Demo