An Analysis of the Tor Handshake

Akhil Kammila
Mentor: Kyle Hogan
Outline

1. Tor Introduction
2. Tor’s Handshake
3. Improvements
Tor Introduction
Anonymity

- Relationship anonymity
Anonymity

- Relationship anonymity

Client ———> Destination
Anonymity

- Relationship anonymity

- Linkable
Normal Internet Connection

Client

Destination
Normal Internet Connection

Client

Destination

Source Address | Destination Address

Data

4
Normal Internet Connection

<table>
<thead>
<tr>
<th>Source Address</th>
<th>Destination Address</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Linkable by anyone viewing the connection ✗
VPN Connection

Client → VPN Server → Destination
VPN Connection

Client → VPN Server → Destination
VPN Connection

- Not linkable by anyone viewing the connection
VPN Connection

- Not linkable by anyone viewing the connection
VPN Connection

- Not linkable by anyone viewing the connection
- Linkable by the VPN server
Tor Internet Connection

Client

Relay

Relay

Relay

Destination
Tor Internet Connection

- Not linkable by anyone viewing the connection
Tor Internet Connection

- Not linkable by anyone viewing the connection
- Not linkable by relays

Client ➔ Relay ➔ Relay ➔ Relay ➔ Destination
Tor Internet Connection

- Not linkable by anyone viewing the connection
- Not linkable by relays
Tor Internet Connection

- Not linkable by anyone viewing the connection
- Not linkable by relays
2 Tor’s Handshake
Why Handshake?

1. Authentication
Why Handshake?

1. Authentication

Normal connection

Client → Destination

Image of a handshake with a wax seal, illustrating the authentication process.
Why Handshake?

1. **Authentication**

**Normal connection**

Client → Destination

**Tor connection**

Client → Relay → Relay → Relay → Destination
Why Handshake?

1. Authentication

Normal connection

Client → Destination

Tor connection

Client ← Relay ← Relay ← Relay ← Destination
Why Handshake?

1. Authentication

Normal connection

Client → Destination

Tor connection

Client → Relay → Relay → Relay → Destination
Why Handshake?

1. Authentication
Why Handshake?

Normal connection

Client → Destination

Tor connection

Client → Relay → Relay → Relay → Destination

1. Authentication
2. Key Exchange
Why Handshake?

1. Authentication
2. Key Exchange
Why Handshake?

1. Authentication
2. Key Exchange

Normal connection

Client ➔ Destination

Tor connection

Client ➔ Relay ➔ Relay ➔ Relay ➔ Destination
Why Handshake?

1. Authentication
2. Key Exchange
Why Handshake?

1. Authentication
2. Key Exchange
Handshakes

Normal

Client

Server

Starting message
Handshakes

Normal

Client

Server

Starting message

1

2
Handshakes

Normal

Client

Server

1. Starting message

2.

3.
Handshakes

Normal

Client

Server

1. Starting message

2.

3.

=
Handshakes

Starting message

1. Client
2. Starting message
3. Server

Key = Lock
Handshakes

Client

Server

1. Starting message

2.

3.

Tor
Handshakes

Starting message

1. Client
2. Server
3. =
Handshakes

1. Client → Server: Starting message
2. Server → Client:
3. Client → Server:
4. Server → Client: Starting message
Handshakes

Tor

1. Client
   - Starting message

2. Server
   - Envelope

3. Client
   - Key
   - Padlock

4. Client
   - Envelope
   - Padlock

5. Server
   - Starting message
   - Padlock
**Handshakes**

**Tor**

1. **Client**

2. **Server**

3. **Client**

4. **Server**

Starting message

5. **Client**

6. **Server**

=
3 Improvements
Improvements

Performance

Round trips
Bandwidth: Data being sent
Improvements

**Performance**
- Round trips
- Bandwidth: Data being sent

**Security**
- Sensitive information being leaked
Removing Handshake Redundancy

Tor

1. Client

2. Server

3. $\text{Starting message}$

4. Client

5. Server

6. $\text{Starting message}$

$\text{Starting message}$
Removing Handshake Redundancy

Tor

Client

Server

1. Starting message

2. 

3. 

4. Starting message

5.

6. 

=
Removing Handshake Redundancy

1. Tor
2. Client
3. Server

Starting message

4. Client
5. Server

Starting message

=
Removing Handshake Redundancy

Tor

Client

Server

Starting message

Performance

Bandwidth: Data being sent

1

2

3

= 

4

5

6
Removing Old Versions of Tor

Version 1
Version 2
Version 3
Removing Old Versions of Tor

Version 1
Version 2
Version 3
Removing Old Versions of Tor

1. Client
2. Server
3. Version 1
   Version 2
   Version 3
4. Client
   Starting message
5. Server
6. =
Removing Old Versions of Tor
Removing Old Versions of Tor

Version 1
Version 2
Version 3
Removing Old Versions of Tor

≈0% lose support
Removing Old Versions of Tor

- Only one Version
- Can use vanilla handshake

≈0% lose support

Version 1
Version 2
Version 3
Removing Old Versions of Tor

- Only one Version
- Can use vanilla handshake
- Reduced Round Trips
- Improved Security

≈0% lose support
Removing Old Versions of Tor

- Only one Version
  - Can use vanilla handshake
  - Reduced Round Trips
  - Improved Security

- ≈0% lose support

Performance
- Round trips

Security
- Sensitive information being leaked
Takeaways

Tor uses relays to achieve anonymity

Tor has a special handshake that hides two-way authentication

We propose 2 improvements to Tor’s handshake
  - Removing extra certificate
  - Removing old versions of Tor
Acknowledgements

Thank you to:
- My Mentor: Kyle Hogan
- Cristina Nita-Rotaru
- PRIMES
- My family