Anonymity on the network

ISSES

Co-funded by the
Erasmus+ Programme
of the European Union

Network traffic anonymization

- Anonymizing network traffic goal: hide the IP address from which someone accesses some service (e.g. web page).
- Simple solution: use a proxy, and the destination will not know the IP address of the communication initiator.
  - Do you trust proxy?
  - Do you trust network hosting proxy?
  - Can the attacker observe proxy communication and correlate incoming and outgoing traffic?

ISSES

Co-funded by the
Erasmus+ Programme
of the European Union

Tor – low latency online anonymization

- High latency anonymity networks (Babel, Mixmaster, Mixminion) not useful for interactive network use
- Tor provides low-latency network traffic anonymization of the interactive network traffic.
- Encryption based anonymization
- Can be used for different services (web, ssh,…) using SOCKS proxy

ISSES

Co-funded by the
Erasmus+ Programme
of the European Union

Tor building blocks

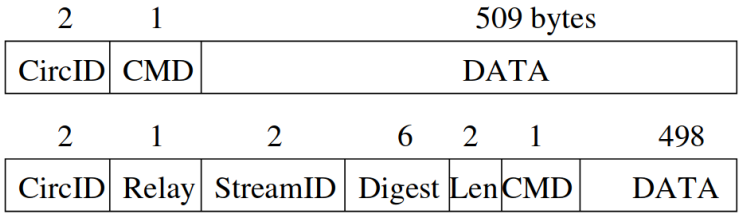
- Client: Tor browser (based on Firefox)
- OR: Onion routers
- Server which is accessed
- Directory server
- OP: Onion proxy: local software on a client which
  - fetches OR directories,
  - establish circuits across the network
  - handle connections from user applications.
  - accept TCP streams and multiplex them across the circuits.

ISSES

Co-funded by the
Erasmus+ Programme
of the European Union

Tor OR and cells

- Has long term private key used to exchange short term keys and sign TLS certificates
- Tor circuit consists of 3 OR chosen by the client
- Each circuit can be used by multiple TCP streams
- All Tor messages are exchanged in 512 bytes cells
  - Control cells (carry control traffic, e.g. key exchanges)
  - Relay cells (carry users traffic)



ISSES
Co-funded by the Erasmus+ Programme of the European Union

Establishing Tor circuit (1)

1. Client OP (Tor browser) chooses OR path
2. Client initiates DH exchange with the first router on the path OR1
3. Symmetric key K_{C1} is created between the client and the OR1
4. Client initiates DH exchange with the OR2. These messages are sent encrypted with the K_{C1} towards the OR1.

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Establishing Tor circuit (2)

5. OR1 decrypts key exchange material for OR2 and relays it towards the OR2 (with OR1 as a source of these messages)
6. OR2 responds with the public DH key towards the OR1 which forwards this message to the Client encrypted with the K_{C1}
7. Key K_{C2} between the Client and OR2 is exchanged. OR2 does not know the IP address of the Client since key exchange messages are relayed by OR1

ISSES

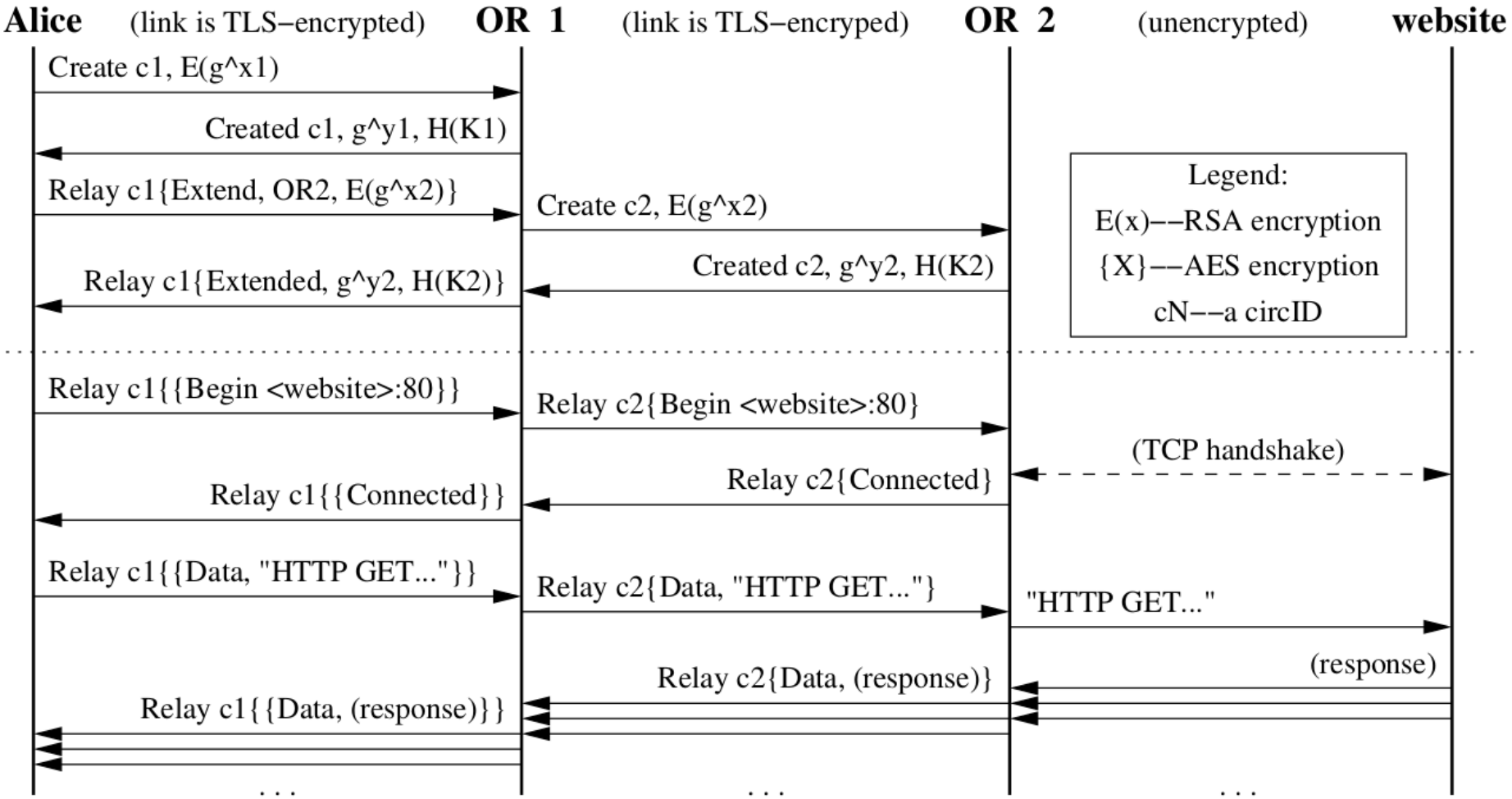
Co-funded by the
Erasmus+ Programme
of the European Union

Establishing Tor circuit (3)

8. Client initiates DH exchange with the OR3. These messages are sent encrypted with the K_{C1} and then K_{C2} and sent towards the OR1
9. OR1 decrypts key exchange material for OR3 and relays it towards the OR2
10. OR2 decrypts key exchange material for OR3 and relays it towards the OR3
11. Key K_{C3} between the Client and OR3 is exchanged. OR3 does not know the IP address of the Client since key exchange messages are relayed by OR2

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Establishing two-OR circuit



ISSES
Co-funded by the
Erasmus+ Programme
of the European Union

Sending Tor messages

- Client creates a message M for the server and sends it in a following way:
  - $E(K_{C1}, E(K_{C2}, E(K_{C3}, M)))$
- OR1 gets the message and decrypts it with the K_{C1} and forwards the message: $E(K_{C2}, E(K_{C3}, M))$
- OR2 gets the message and decrypts it with the K_{C2} and forwards the message: $E(K_{C3}, M)$
- OR3 gets the message and decrypts it with the K_{C3} and forwards the message to the server.

ISSES

Co-funded by the
Erasmus+ Programme
of the European Union

Tor routing summary

- OR1 communicates with the Client and OR2
- OR2 communicates with the OR1 and OR3
- OR3 communicates with the OR2 and the server
- Message is seen only by Client, Server and OR3 (can be encrypted in case of the TLS connection)
- OR2, OR3 and server do not know the IP address of the client

ISSES

Co-funded by the
Erasmus+ Programme
of the European Union

Hidden (.onion) services

- Opposite problem – how to hide service location (e.g. web server IP address)
- Server has .onion domain (e.g.: http://3g2upl4pq6kufc4m.onion/)
- Names are opaque strings generated from public keys
- .onion is not a actual DNS domain (not in the internet DNS root). Cannot be resolved with DNS queries
- .onion sites can be accessed only from the Tor network

ISSES

Co-funded by the Erasmus+ Programme of the European Union

Creating hidden service

- Path is 6 OR long: Client-RP (3 OR) + RP-Server (3 OR)

1. Server generates a long-term public key pair to identify his service.
2. Server chooses some **introduction points** (OR), and advertises them on the lookup service (e.g. web page), signing the advertisement with his public key.
3. Server builds a circuit to each of his introduction points, and tells them to wait for requests.

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Accessing the hidden service (1)

1. Client learns about Servers service out of band.
2. Client retrieves the details of Servers service from the lookup service.
3. If Client wants to access Servers service anonymously, she must connect to the lookup service via Tor
4. Client chooses an OR as the **rendezvous point** (RP) for her connection to Servers service.
5. Client builds a circuit to the RP, and gives it a randomly chosen "**rendezvous cookie**" to recognize Server.

ISSES

Co-funded by the
Erasmus+ Programme
of the European Union

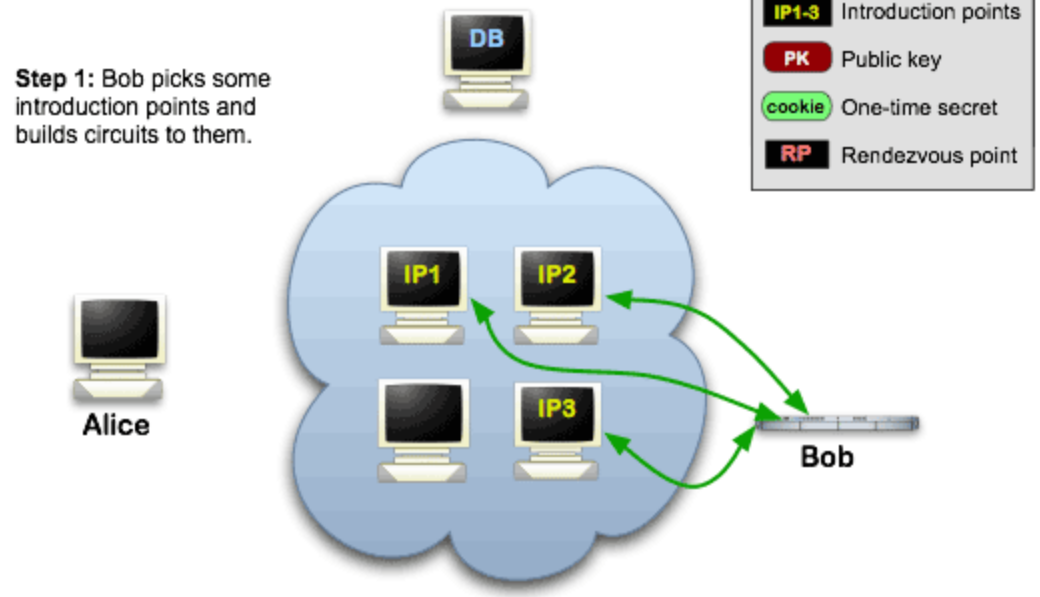
Accessing the hidden service (2)

6. Client opens an anonymous stream to one of Servers introduction points, and gives it a message (encrypted with Servers public key) telling it about client, his RP and rendezvous cookie, and the start of a DH handshake.
7. The introduction point sends the message to Server.
8. If Server wants to talk to Client, he builds a circuit to Clients RP and sends the rendezvous cookie, the second half of the DH handshake, and a hash of the session key they now share.
9. The RP connects Clients circuit to Servers. RP can't recognize Client, Server, or the data they transmit.
10. Client sends a relay begin cell along the circuit. It arrives at Servers OP, which connects to Server.
11. An anonymous stream has been established, and Client and Server communicate as normal.

ISSES

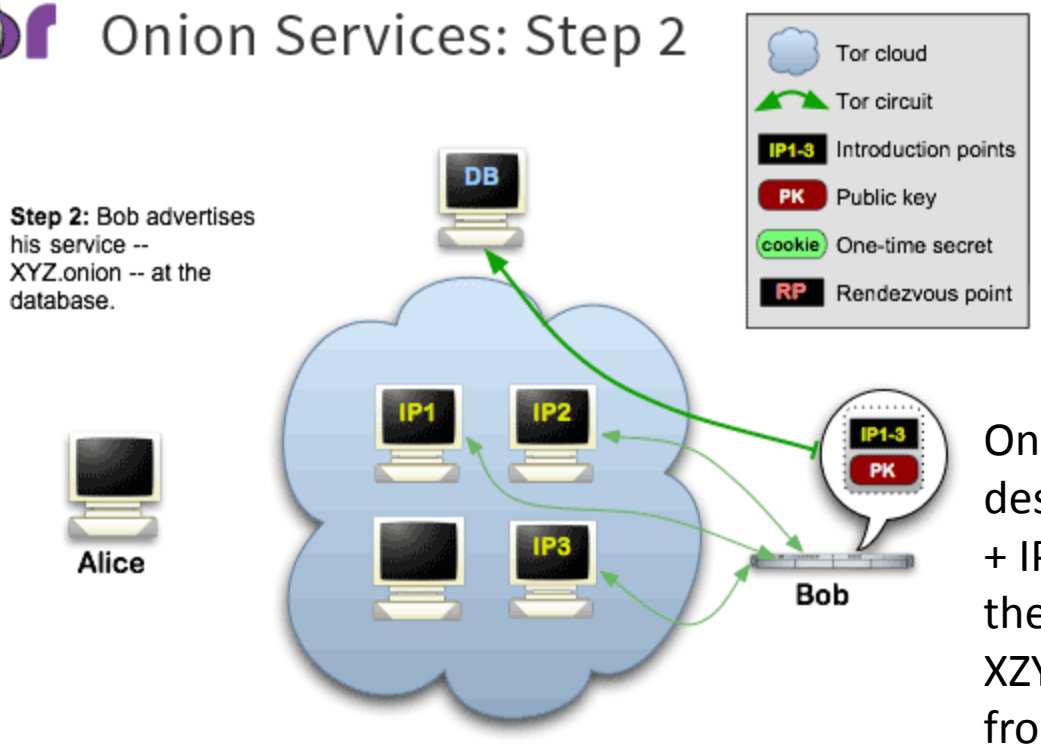
Co-funded by the
Erasmus+ Programme
of the European Union

Onion Services: Step 1



ISSES
Co-funded by the Erasmus+ Programme of the European Union

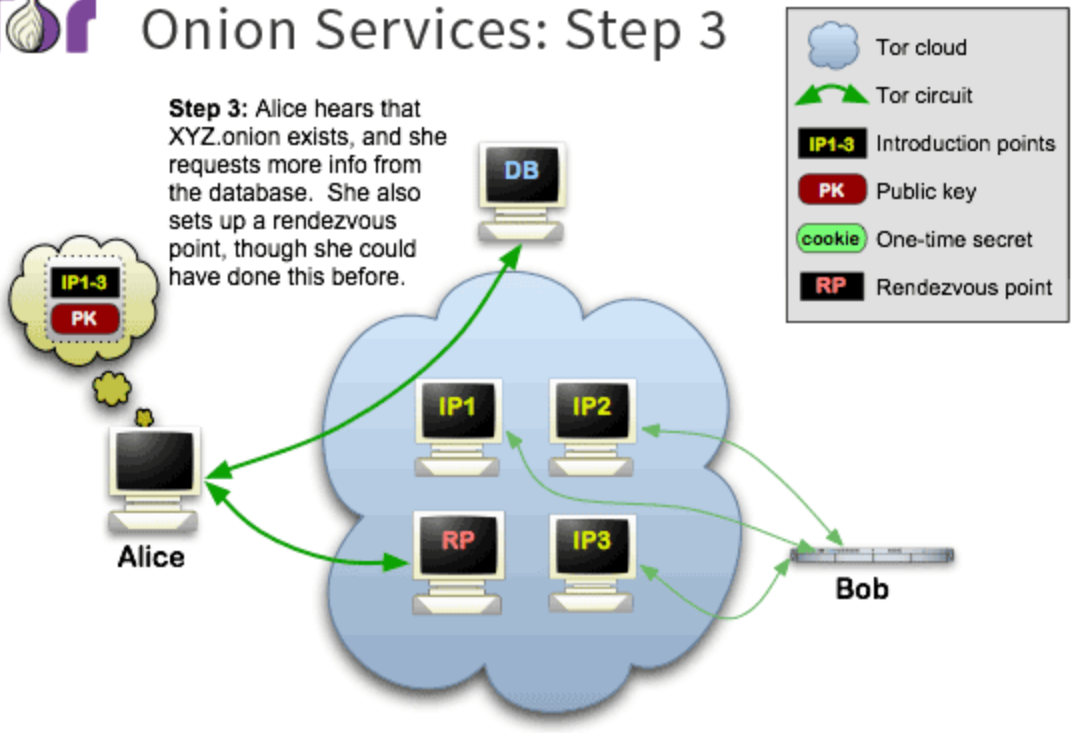
Onion Services: Step 2



Onion service descriptor (public key + IP1-3) signed with the service private key XZY.onion XYZ derived from the public key

ISSES
Co-funded by the Erasmus+ Programme of the European Union

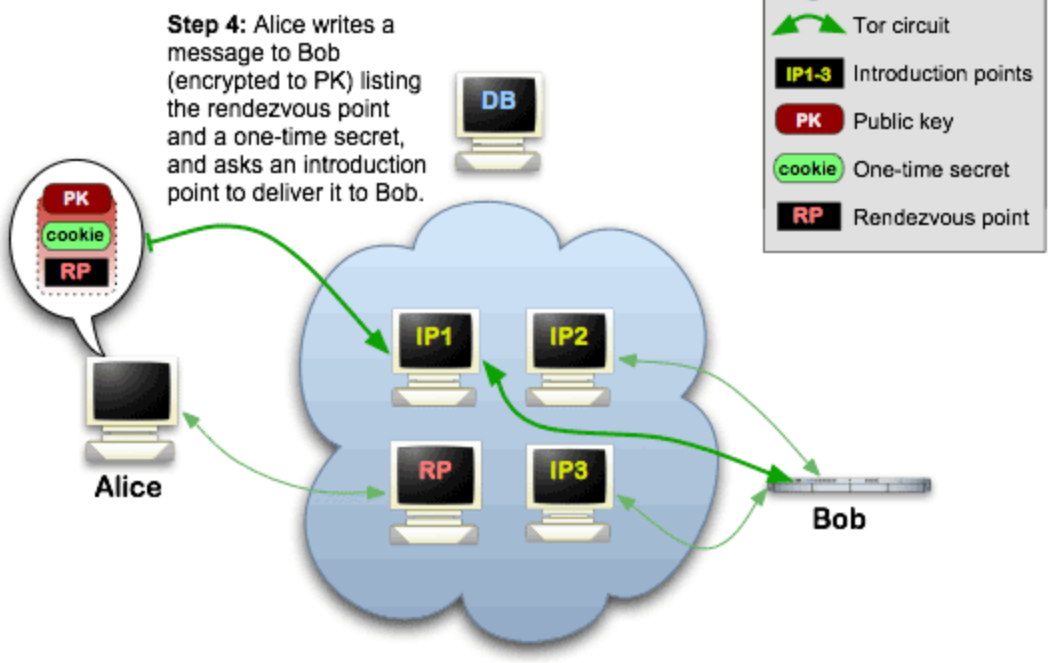
Onion Services: Step 3



ISSES

Co-funded by the Erasmus+ Programme of the European Union

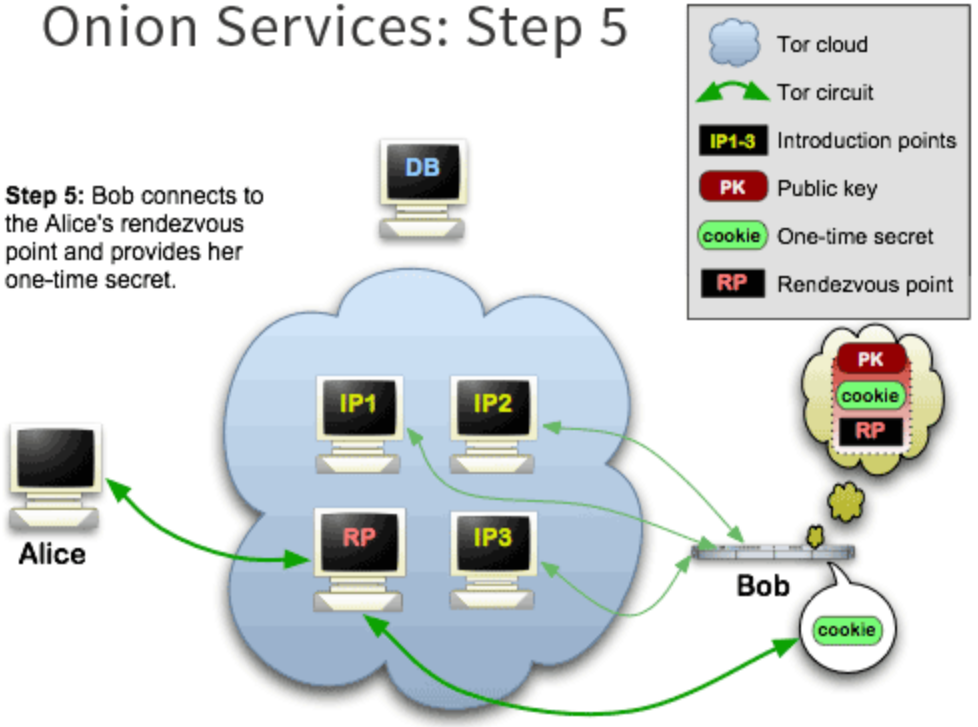
Onion Services: Step 4



ISSES

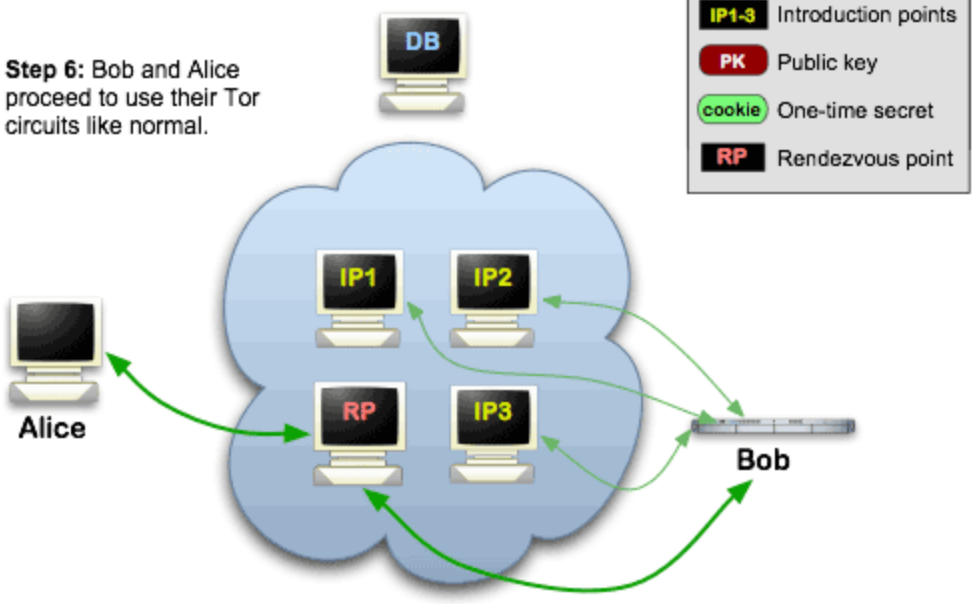
Co-funded by the Erasmus+ Programme of the European Union

Onion Services: Step 5



ISSES
Co-funded by the Erasmus+ Programme of the European Union

Onion Services: Step 6



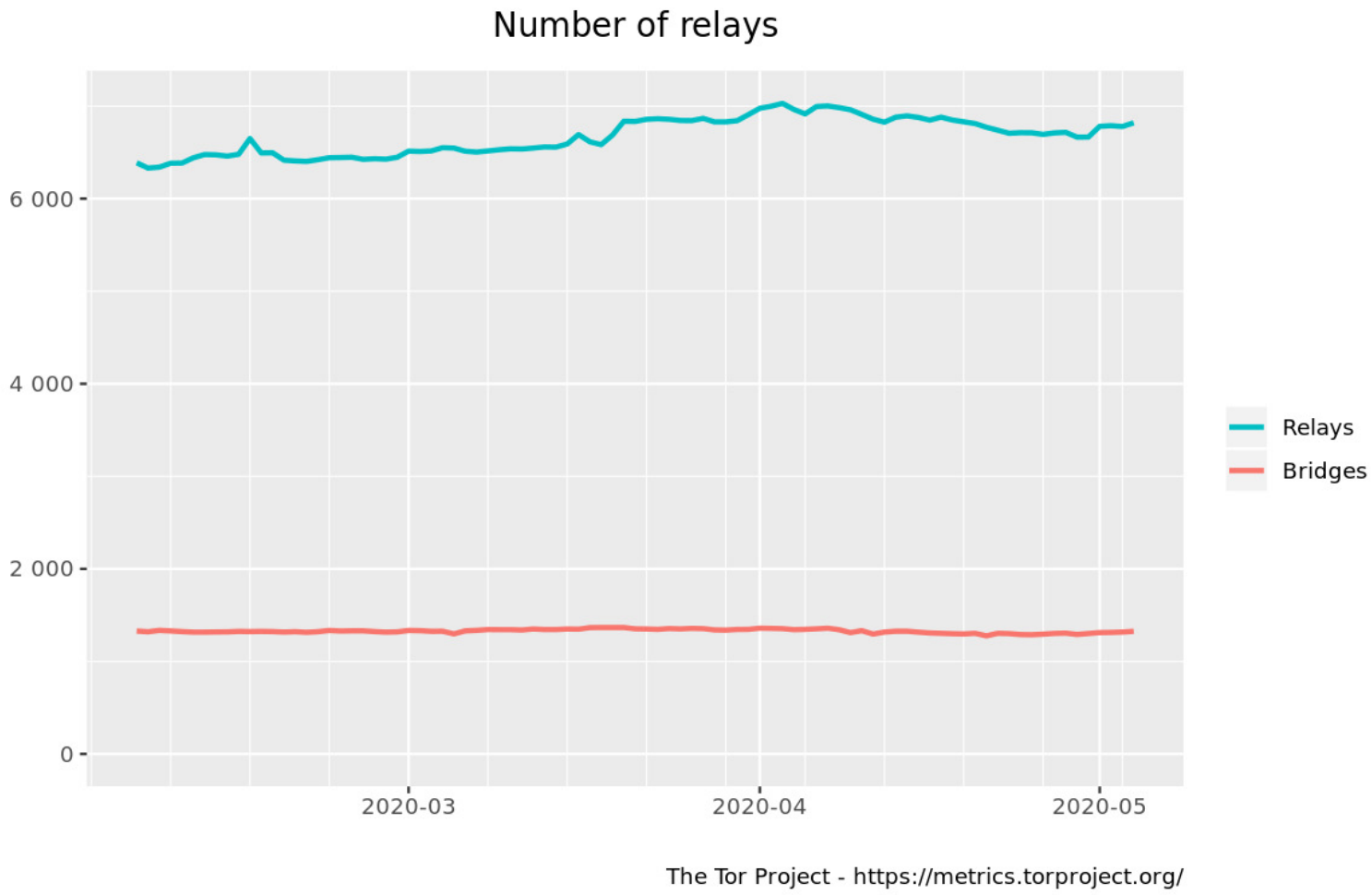
ISSES
Co-funded by the Erasmus+ Programme of the European Union

Size of the Tor network

- April 2019:
  - 2.000.000 users (criminals, hackers, hacktivists, those who don't want to be tracked)
  - More than 6.000 servers
  - Bandwidth 150 Gbps
  - More than 100.000 .onion services (2015 - 30% illicit: 15.4% drugs related, 9% frauds, guns, gambling, abuse, etc.)

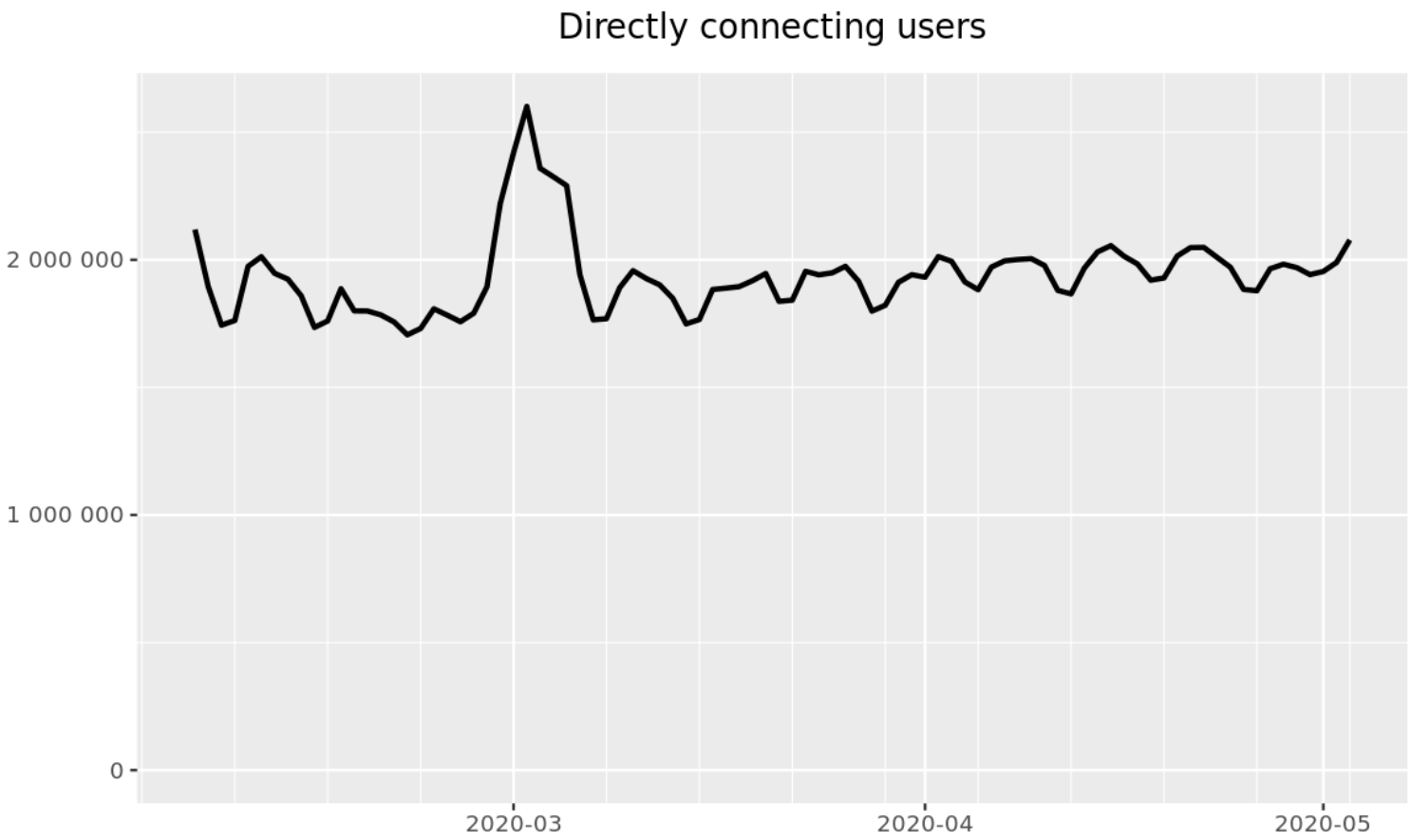
ISSES
Co-funded by the Erasmus+ Programme of the European Union

Number of Tor relays



ISSES
Co-funded by the
Erasmus+ Programme
of the European Union

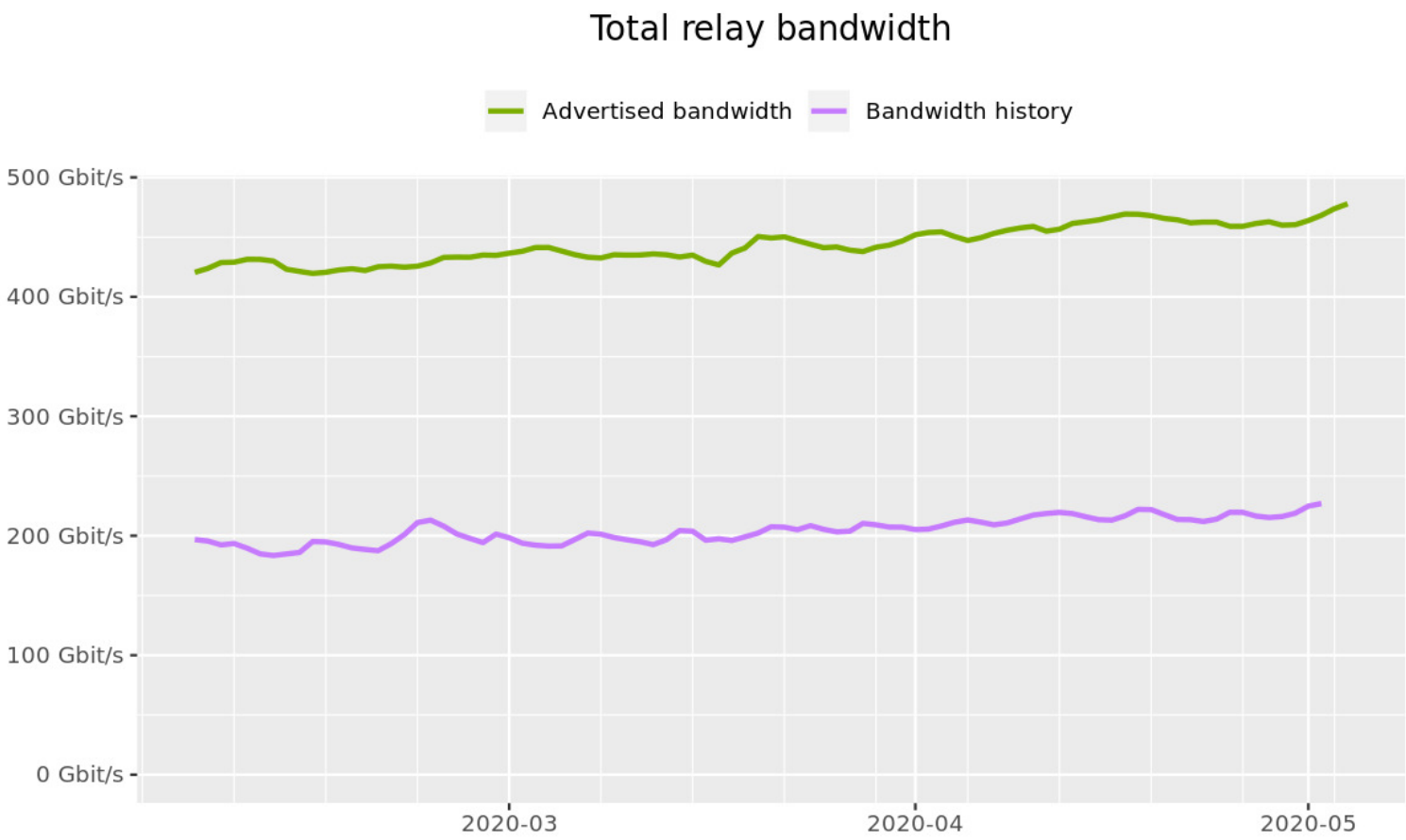
Number of Tor users



The Tor Project - https://metrics.torproject.org/

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Tor throughput

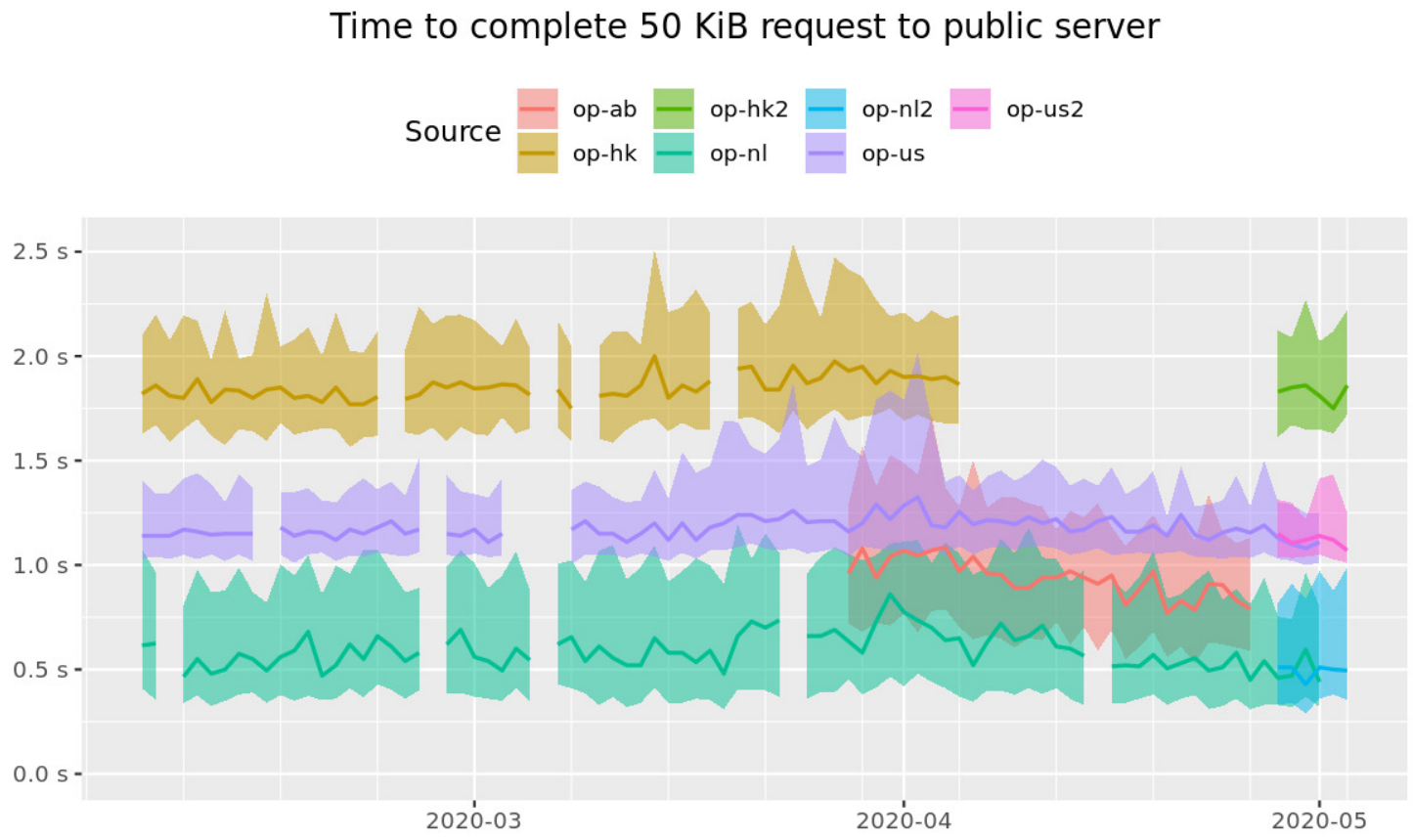


The Tor Project - https://metrics.torproject.org/

ISSES

Co-funded by the
Erasmus+ Programme
of the European Union

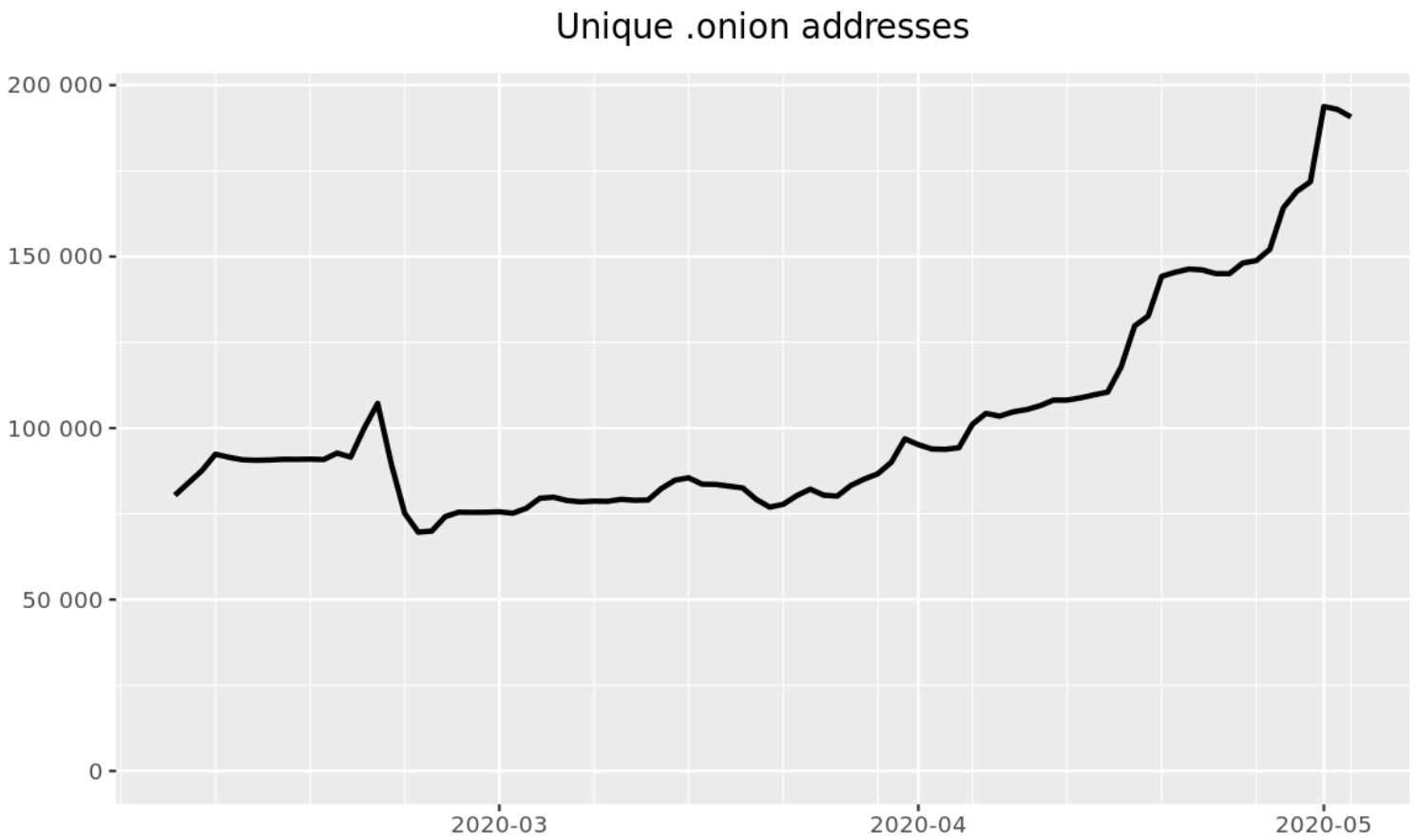
Tor performance



The Tor Project - https://metrics.torproject.org/

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Number of .onion domains



The Tor Project - https://metrics.torproject.org/

ISSES

Co-funded by the Erasmus+ Programme of the European Union

Attacks on Tor network

- Who owns ORs? Can you trust OR owners, do they cooperate? Hostile Ors.
- End-to-end attack: Observing the traffic on the client and server side and correlating the packet patterns
- DoS attack – Ors do the double encryption
- Shut down directory servers, add hostile Ors to the directory
- RP attacks

ISSES

Co-funded by the
Erasmus+ Programme
of the European Union