Privacy methods.

Simulazione di Sistemi

September 11, 2015

Davide Berardi 0000712698

Matteo Martelli 0000702472

Università di Bologna.

Privacy

Anonymity

Anonymity and privacy

But...who cares?

Surveillance

NSA projects

Other stories

Obscuration

Industrial espionage

Not only powerful adversaries

Technologies

Confidentiality and authenticity

Anonymity

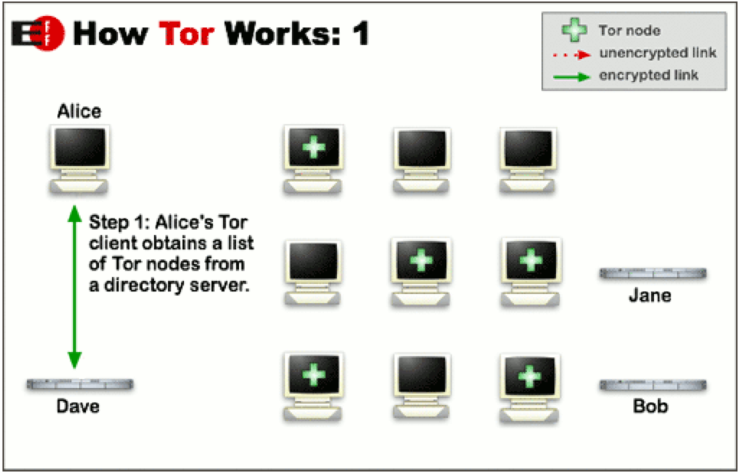
Onion Routing

NSA and Tor

The Tor revolution

Tor

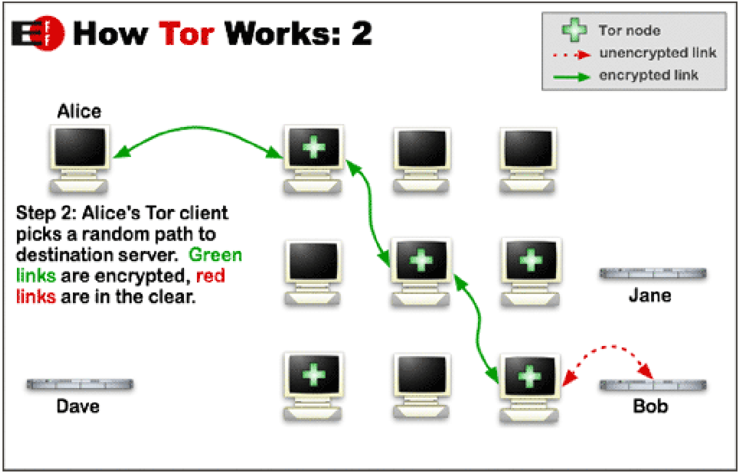
Tor workings



Step 1: Alice's Tor client obtains a list of Tor nodes from a directory server.

Tor

Tor workings

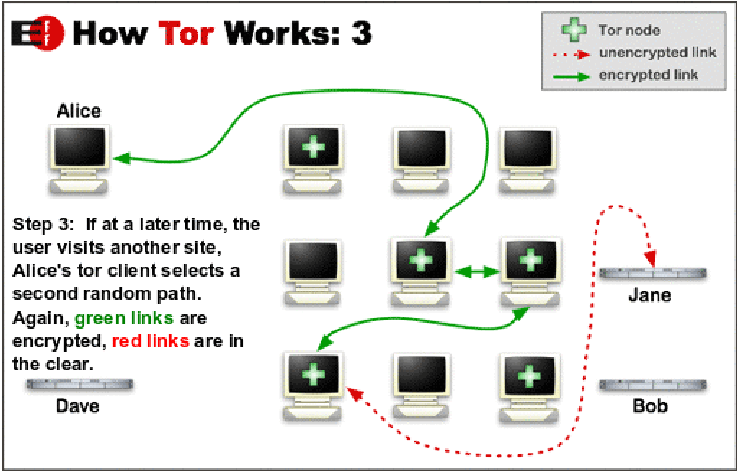


How Tor Works: 2

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

Tor

Tor workings

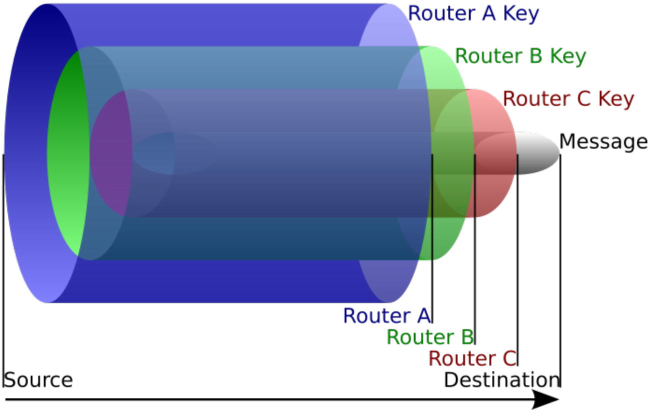


How Tor Works: 3

Step 3: If at a later time, the user visits another site, Alice's tor client selects a second random path. Again, green links are encrypted, red links are in the clear.

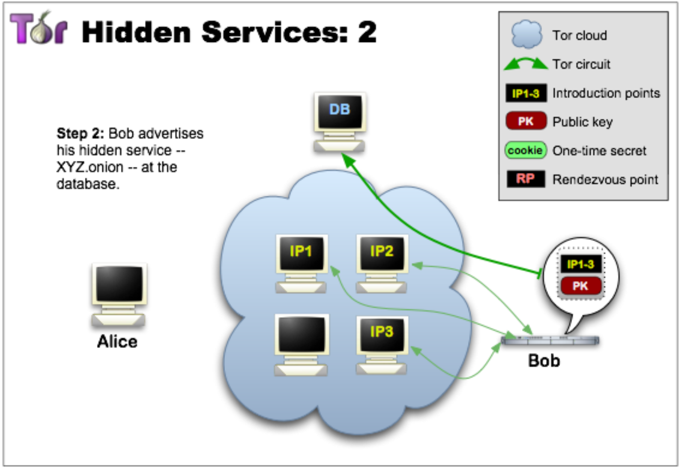
Tor

Tor encryption



Tor

Tor Hidden Service

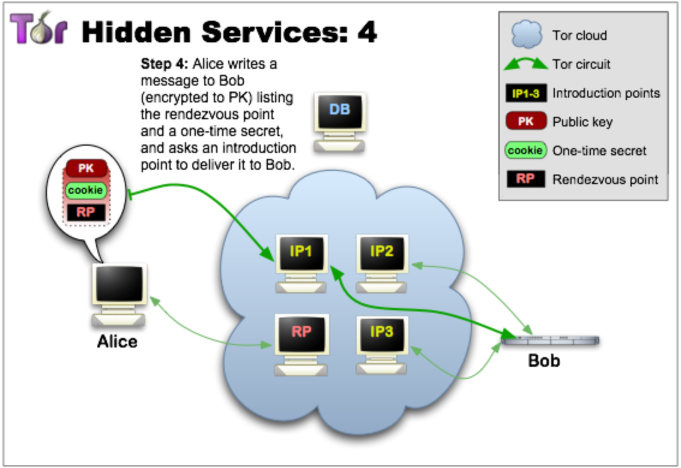


Hidden Services: 2

Step 2: Bob advertises his hidden service -- XYZ.onion -- at the database.

Tor

Tor Hidden Service

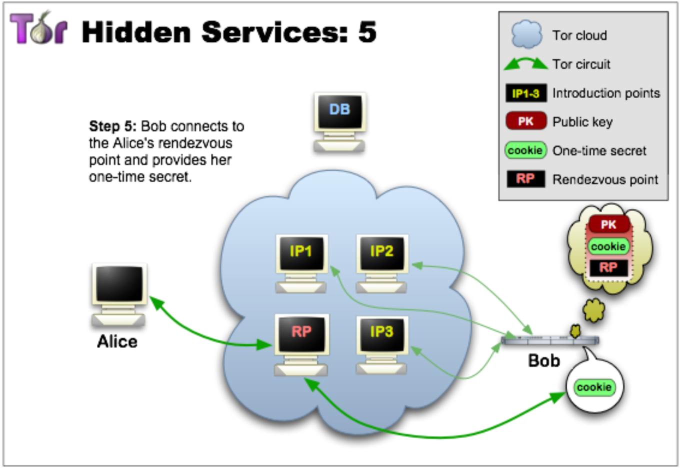


Tor Hidden Services: 4

Step 4: Alice writes a message to Bob (encrypted to PK) listing the rendezvous point and a one-time secret, and asks an introduction point to deliver it to Bob.

Tor

Tor Hidden Service

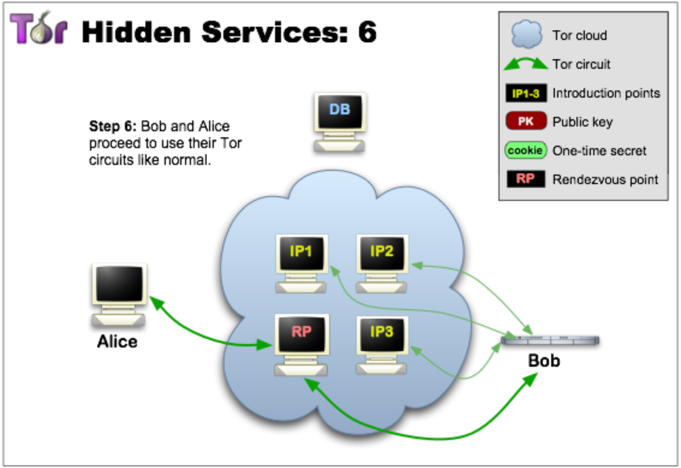


Hidden Services: 5

Step 5: Bob connects to the Alice's rendezvous point and provides her one-time secret.

Tor

Tor Hidden Service



Hidden Services: 6

Step 6: Bob and Alice proceed to use their Tor circuits like normal.

Tor

Summary

- Base: anonimity of clients
- Hidden services: anonimity of client + anonimity of servers

But ... is it enough?"

Time analysis based attacks

> *"Tor does not provide protection against end-to-end timing attacks[...]"*

We can place a tracker after the client node and another before the server node and check for the connection time to profile users and nodes (and later associate IP to users.)

Thank you for your attention.