Privacy methods.

Simulazione di Sistemi

September 12, 2015

Davide Berardi 0000712698

Matteo Martelli 0000702472

Università di Bologna.

Privacy

Privacy is the right to publish only some informations that we want to publish.
There are a lot of laws and legal issues related to privacy (but some people are just not intrested in laws).

Anonymity

We will talk about anonimy as the propriety of disconnect the user of a service from some basic proprieties:

- Geolocation.
- Association to a face or a name (or to an IP address).

Sometimes we need to reassociate the user with a communication channel or so.

But...who cares?

"I have nothing to hide, who cares about my personal data?"

Surveillance

NSA projects

Other stories

Obscuration

Industrial espionage

Not only powerful adversaries

Technologies

Confidentiality and authenticity

We have a lot of programs to protect our data

- PGP
- Protonmail
- IPsec
- OTR-based programs

Anonymity

But for anonymity?

- Mix Max networks.
- Anonymous remailers.
- Proxy chains.
- **Anonymous networks**
- **Onion Routers**

Anonymous network

Onion Routing

NSA and Tor

The Tor revolution

Why simulation?

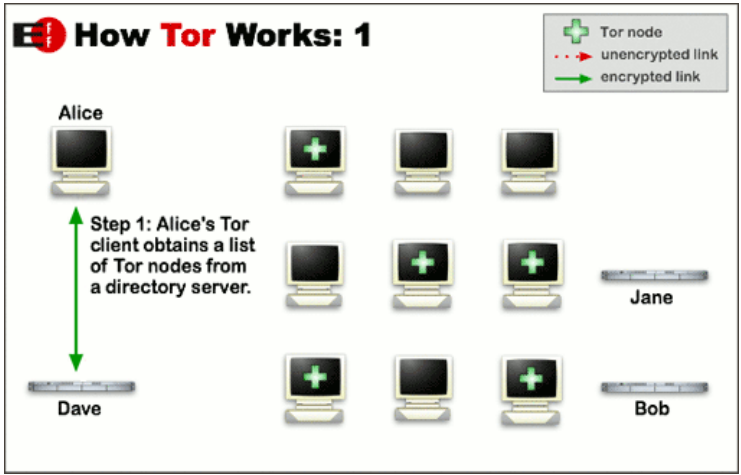
Simulation help us in a lot of aspects:

- Compare the performances of two onion routers (p.e. i2p vs Tor).
- To compare effects of changes in the node choice algorithms.
- **Get an idea of the number of resources needed by an attacker and to mantain anonimity**.

Part 2 – Onion routers and attacks

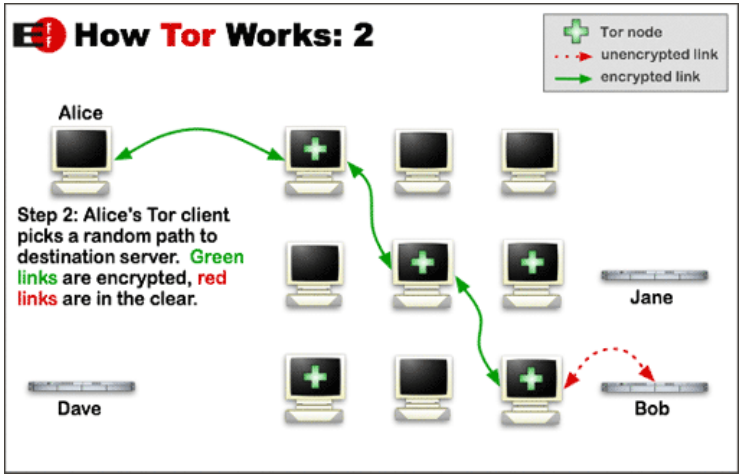
Tor

Tor workings

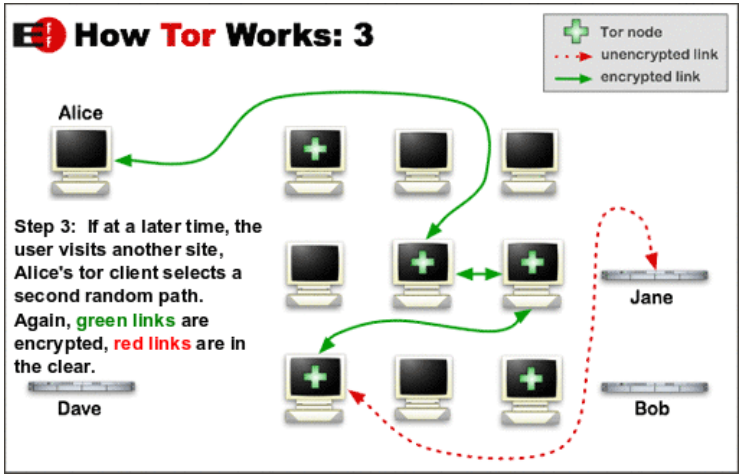


Tor

Tor workings

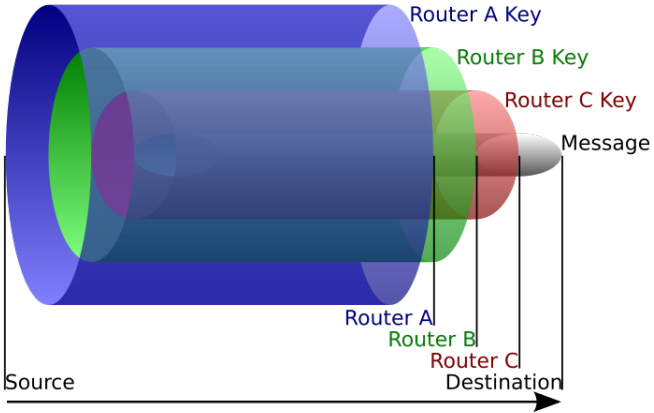


Tor
Tor workings



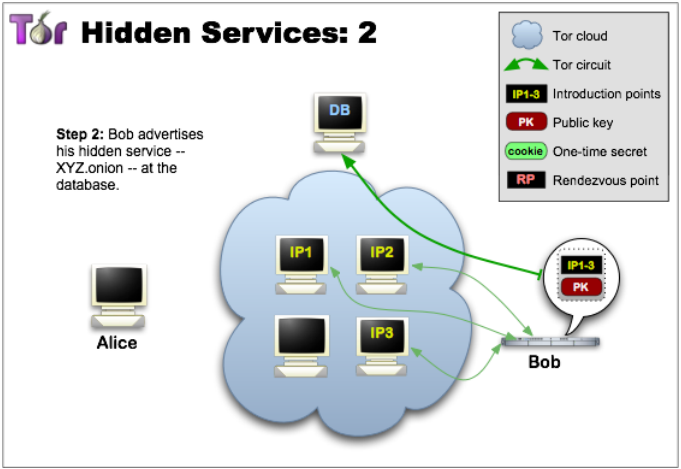
Tor

Tor encryption



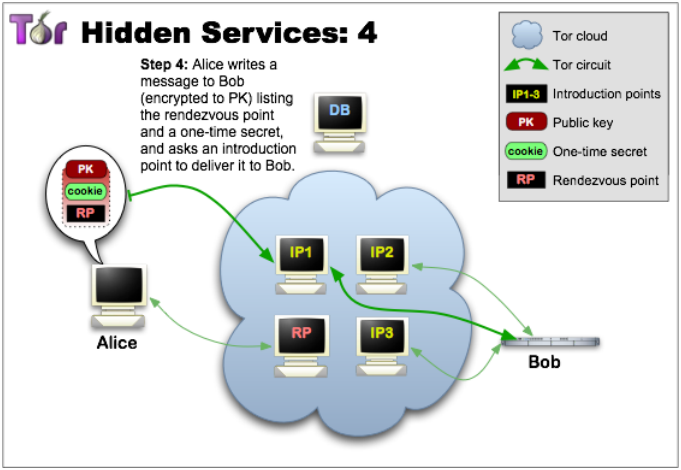
Tor

Tor Hidden Service



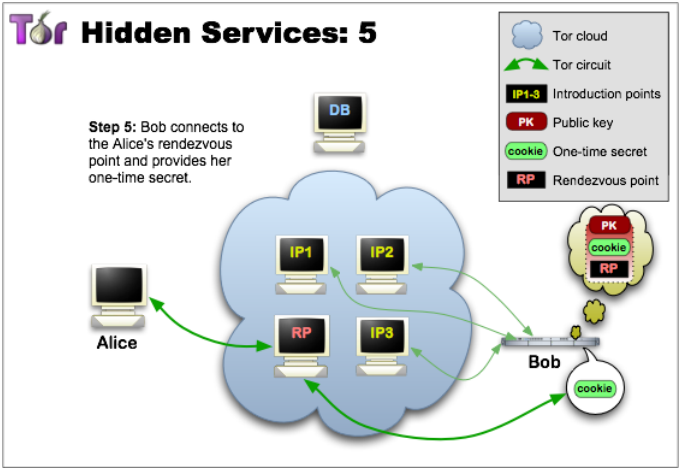
Tor

Tor Hidden Service



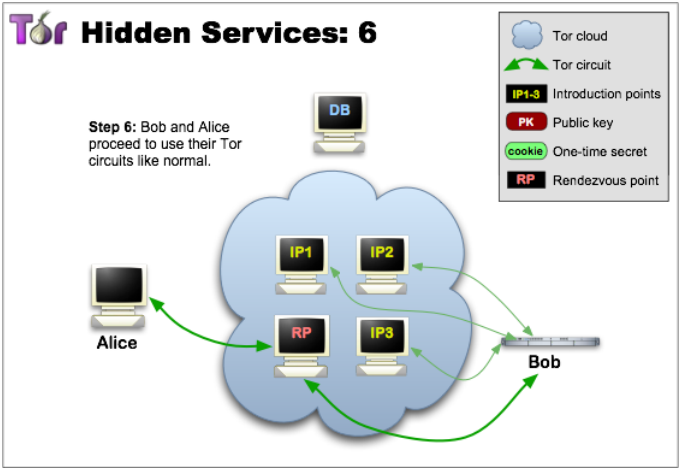
Tor

Tor Hidden Service



Tor

Tor Hidden Service



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.

Diffie-Hellman

- Alice pick a random number a, a prime number p and α as a primitive root of p.
- Alice calculate $k_a = \alpha^a mod p$ and sends $< k_a, p, \alpha >$ over the channel.
- Bob read the packet, pick a random number b, calculate $k_b = \alpha^b mod p$ and sends it to Alice.

Now the shared key $K = k_b^a = k_a^b = \alpha^{ab} mod p$ is known to Alice and Bob[1].

[1] For the little Fermat theorem ($a^p \equiv a \; mod p$) if p is a prime

Perfect Forward Secrecy

- If a key is derived from another with a deterministic method then a leak of the second key can reveal every eavesdropped transmission encrypthed with the first key.
- The immunity to this kind of attacks is called *Perfect Forward Security*.
- Used in Diffie Hellman based TLS, OTR, etc.

Freenet