

Privacy methods.

Simulazione di Sistemi

September 12, 2015

Davide Berardi
0000712698

Matteo Martelli
0000702472

Università di Bologna.





Privacy

Privacy methods.

Davide Berardi,
Matteo Martelli

Introduction

1

Who's involved?

Surveillance
Obscuring
Companies
Bad Guys

Programs

Tor

Timing Attack

Astoria

Other ORs and technologies

HORNET

Open Problems

Simulazione di Sistemi

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

Privacy methods.

Davide Berardi,
Matteo Martelli

Introduction

2

Who's involved?

Surveillance
Obscuring
Companies
Bad Guys

Programs

Tor

Timing Attack

Astoria

Other ORs and technologies

HORNET

Open Problems

Simulazione di Sistemi

We will talk about anonymity 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?

Privacy methods.

Davide Berardi,
Matteo Martelli

Introduction

Who's involved?

3

Surveillance

Obscuring

Companies

Bad Guys

Programs

Tor

Timing Attack

Astoria

Other ORs and
technologies

HORNET

Open Problems

Simulazione di Sistemi

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



Surveillance

Privacy methods.

Davide Berardi,
Matteo Martelli

Introduction

Who's involved?

Surveillance

Obscuring

Companies

Bad Guys

Programs

Tor

Timing Attack

Astoria

Other ORs and technologies

HORNET

Open Problems

Simulazione di Sistemi

4



NSA projects

Privacy methods.

Davide Berardi,
Matteo Martelli

Introduction

Who's involved?

Surveillance

Obscuring

Companies

Bad Guys

Programs

Tor

Timing Attack

Astoria

Other ORs and technologies

HORNET

Open Problems

Simulazione di Sistemi

5



Other stories

Privacy methods.

Davide Berardi,
Matteo Martelli

Introduction

Who's involved?

Surveillance

Obscuring

Companies

Bad Guys

Programs

Tor

Timing Attack

Astoria

Other ORs and technologies

HORNET

Open Problems

Simulazione di Sistemi

6



Obscuration

Privacy methods.

Davide Berardi,
Matteo Martelli

Introduction

Who's involved?

Surveillance

Obscuring

Companies

Bad Guys

7

Programs

Tor

Timing Attack

Astoria

Other ORs and technologies

HORNET

Open Problems

Simulazione di Sistemi



Industrial espionage

Privacy methods.

Davide Berardi,
Matteo Martelli

Introduction

Who's involved?

Surveillance

Obscuring

Companies

Bad Guys

Programs

Tor

Timing Attack

Astoria

Other ORs and technologies

HORNET

Open Problems

Simulazione di Sistemi

8



Not only powerful adversaries

Privacy methods.

Davide Berardi,
Matteo Martelli

Introduction

Who's involved?

Surveillance

Obscuring

Companies

Bad Guys

9

Programs

Tor

Timing Attack

Astoria

Other ORs and technologies

HORNET

Open Problems

Simulazione di Sistemi



Technologies

Privacy methods.

Davide Berardi,
Matteo Martelli

Introduction

Who's involved?

Surveillance
Obscuring
Companies
Bad Guys

Programs

10

Tor

Timing Attack

Astoria

Other ORs and technologies

HORNET

Open Problems

Simulazione di Sistemi



Confidentiality and authenticity

Privacy methods.

Davide Berardi,
Matteo Martelli

Introduction

Who's involved?

Surveillance
Obscuring
Companies
Bad Guys

Programs

11

Tor

Timing Attack

Astoria

Other ORs and technologies

HORNET

Open Problems

Simulazione di Sistemi

We have a lot of programs to protect our data

- ▶ PGP
- ▶ Protonmail
- ▶ IPsec
- ▶ OTR-based programs



Anonymity

Privacy methods.

Davide Berardi,
Matteo Martelli

Introduction

Who's involved?

Surveillance
Obscuring
Companies
Bad Guys

Programs

12

Tor

Timing Attack

Astoria

Other ORs and technologies

HORNET

Open Problems

Simulazione di Sistemi

But for anonymity?

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



Anonymous network

Privacy methods.

Davide Berardi,
Matteo Martelli

Introduction

Who's involved?

Surveillance
Obscuring
Companies
Bad Guys

Programs

13

Tor

Timing Attack

Astoria

Other ORs and technologies

HORNET

Open Problems

Simulazione di Sistemi



Onion Routing

Privacy methods.

Davide Berardi,
Matteo Martelli

Introduction

Who's involved?

Surveillance
Obscuring
Companies
Bad Guys

Programs

14

Tor

Timing Attack

Astoria

Other ORs and technologies

HORNET

Open Problems

Simulazione di Sistemi



NSA and Tor

Privacy methods.

Davide Berardi,
Matteo Martelli

Introduction

Who's involved?

Surveillance
Obscuring
Companies
Bad Guys

Programs

Tor

15

Timing Attack

Astoria

Other ORs and technologies

HORNET

Open Problems

Simulazione di Sistemi



The Tor revolution

Privacy methods.

Davide Berardi,
Matteo Martelli

Introduction

Who's involved?

Surveillance

Obscuring

Companies

Bad Guys

Programs

Tor

16

Timing Attack

Astoria

Other ORs and technologies

HORNET

Open Problems

Simulazione di Sistemi



Why simulation?

Privacy methods.

Davide Berardi,
Matteo Martelli

Introduction

Who's involved?

Surveillance
Obscuring
Companies
Bad Guys

Programs

Tor

Timing Attack

Astoria

Other ORs and technologies

HORNET

Open Problems

Simulazione di Sistemi

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 maintain anonymity.**

17

Part 2 – Onion routers and attacks





Tor

Tor workings

Privacy methods.

Davide Berardi,
Matteo Martelli

Introduction

Who's involved?

Surveillance
Obscuring
Companies
Bad Guys

Programs

Tor

Timing Attack

Astoria

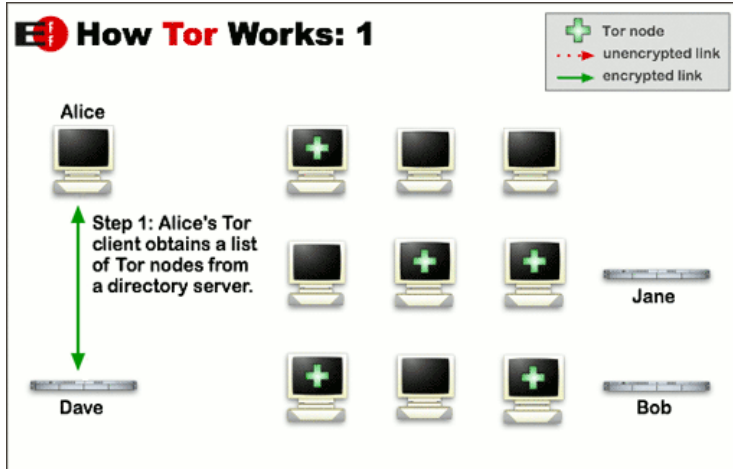
Other ORs and technologies

HORNET

Open Problems

Simulazione di Sistemi

18





Tor

Tor workings

Privacy methods.

Davide Berardi,
Matteo Martelli

Introduction

Who's involved?

Surveillance
Obscuring
Companies
Bad Guys

Programs

Tor

Timing Attack

Astoria

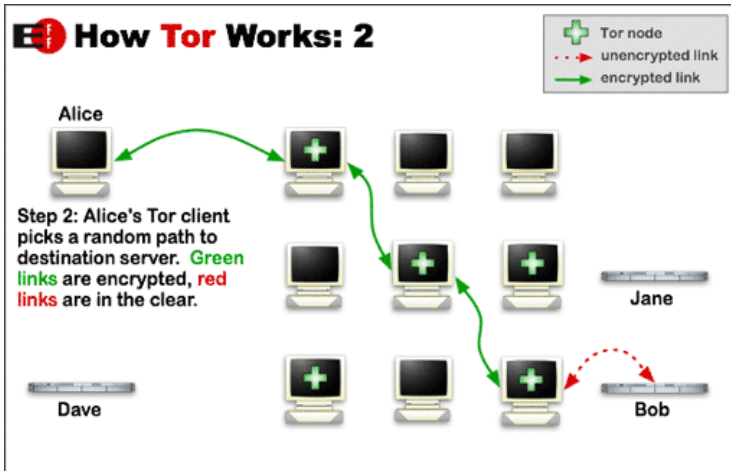
Other ORs and technologies

HORNET

Open Problems

Simulazione di Sistemi

19





Tor

Tor workings

Privacy methods.

Davide Berardi,
Matteo Martelli

Introduction

Who's involved?

Surveillance
Obscuring
Companies
Bad Guys

Programs

Tor

20

Timing Attack

Astoria

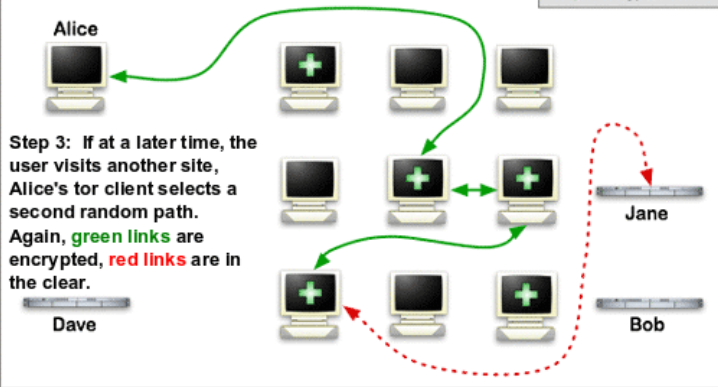
Other ORs and technologies

HORNET

Open Problems

Simulazione di Sistemi

How Tor Works: 3





Tor

Tor encryption

Privacy methods.

Davide Berardi,
Matteo Martelli

Introduction

Who's involved?

Surveillance
Obscuring
Companies
Bad Guys

Programs

Tor

Timing Attack

Astoria

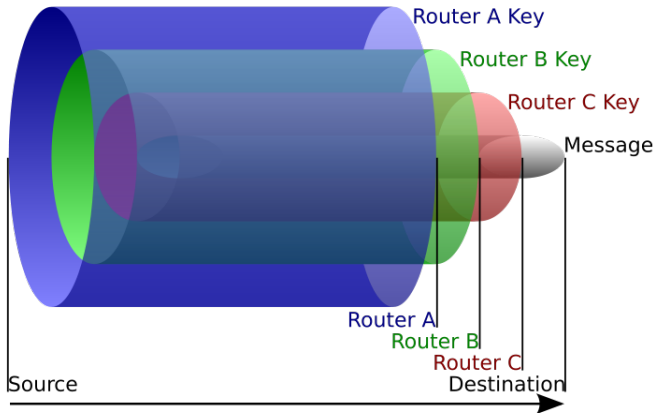
Other ORs and technologies

HORNET

Open Problems

Simulazione di Sistemi

21





Tor

Tor Hidden Service

Privacy methods.

Davide Berardi,
Matteo Martelli

Introduction

Who's involved?

Surveillance
Obscuring
Companies
Bad Guys

Programs

Tor

Timing Attack

Astoria

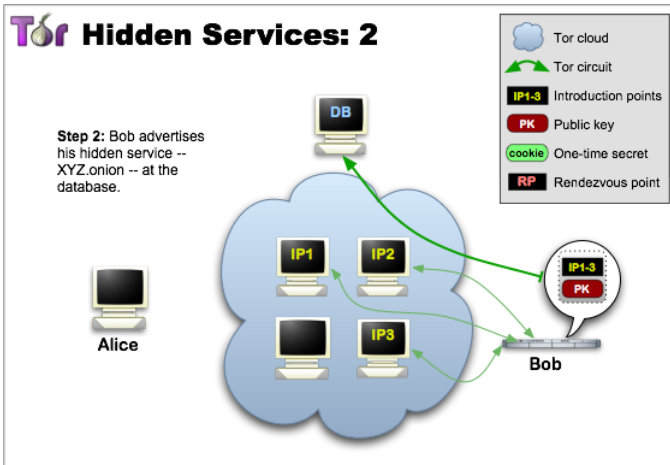
Other ORs and technologies

HORNET

Open Problems

Simulazione di Sistemi

22





Tor

Tor Hidden Service

Privacy methods.

Davide Berardi,
Matteo Martelli

Introduction

Who's involved?

Surveillance

Obscuring

Companies

Bad Guys

Programs

Tor

Timing Attack

Astoria

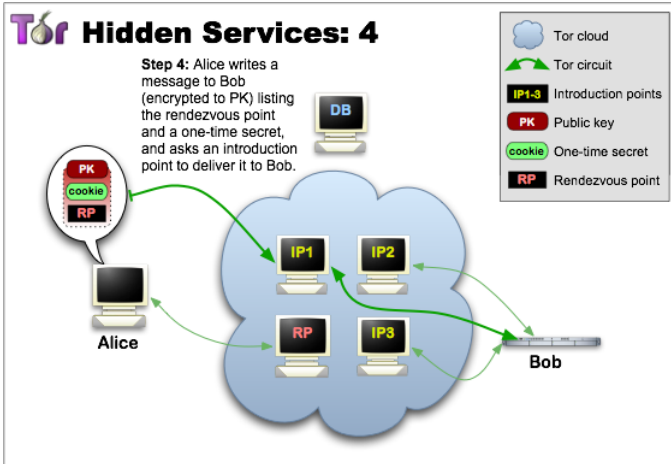
Other ORs and
technologies

HORNET

Open Problems

Simulazione di Sistemi

23





Tor

Tor Hidden Service

Privacy methods.

Davide Berardi,
Matteo Martelli

Introduction

Who's involved?

Surveillance
Obscuring
Companies
Bad Guys

Programs

Tor

Timing Attack

Astoria

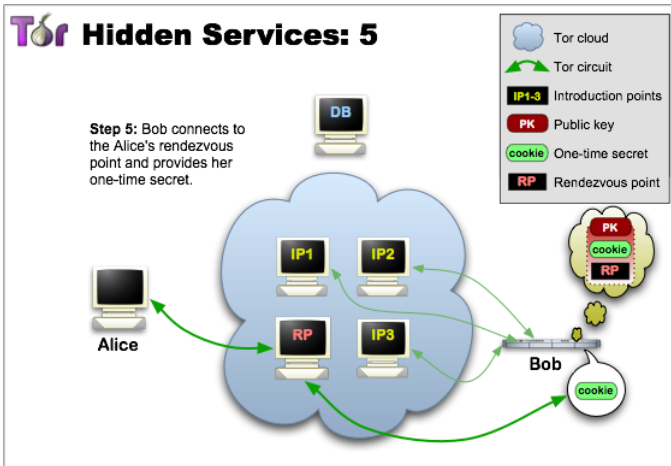
Other ORs and technologies

HORNET

Open Problems

Simulazione di Sistemi

24





Tor

Tor Hidden Service

Privacy methods.

Davide Berardi,
Matteo Martelli

Introduction

Who's involved?

Surveillance
Obscuring
Companies
Bad Guys

Programs

Tor

Timing Attack

Astoria

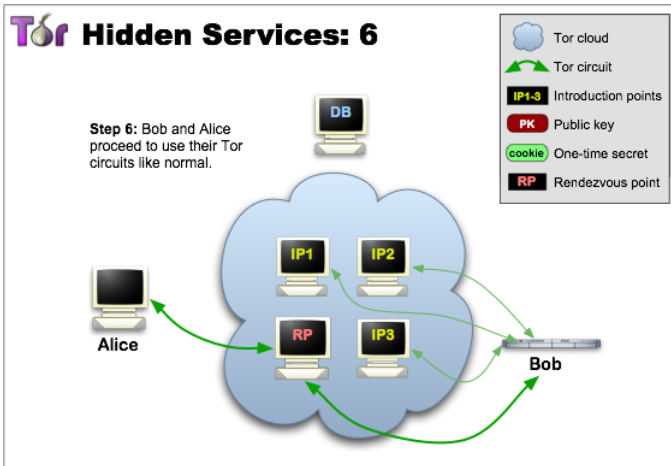
Other ORs and technologies

HORNET

Open Problems

Simulazione di Sistemi

25





Tor

Summary

Privacy methods.

Davide Berardi,
Matteo Martelli

Introduction

Who's involved?

Surveillance
Obscuring
Companies
Bad Guys

Programs

Tor

26

Timing Attack

Astoria

Other ORs and technologies

HORNET

Open Problems

Simulazione di Sistemi

- ▶ Base: anonymity of clients
- ▶ Hidden services: anonymity of client + anonymity of servers

But ... is it enough?"



Time analysis based attacks

Privacy methods.

Davide Berardi,
Matteo Martelli

Introduction

Who's involved?

Surveillance
Obscuring
Companies
Bad Guys

Programs

Tor

Timing Attack

27

Astoria

Other ORs and technologies

HORNET

Open Problems

Simulazione di Sistemi

“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

Privacy methods.

Davide Berardi,
Matteo Martelli

Introduction

Who's involved?

Surveillance
Obscuring
Companies
Bad Guys

Programs

Tor

Timing Attack

Astoria

Other ORs and technologies

HORNET

Open Problems

27

Simulazione di Sistemi

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

Now the shared key $K = k_b^a = k_a^b = \alpha^{ab} \bmod p$ is known to Alice and Bob¹.

¹For the little Fermat theorem ($a^p \equiv a \bmod p$) if p is a prime



Perfect Forward Secrecy

Privacy methods.

Davide Berardi,
Matteo Martelli

Introduction

Who's involved?

Surveillance
Obscuring
Companies
Bad Guys

Programs

Tor

Timing Attack

Astoria

Other ORs and technologies

HORNET

Open Problems

27

Simulazione di Sistemi

- ▶ If a key is derived from another with a deterministic method then a leak of the second key can reveal every eavesdropped transmission encrypted 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

Privacy methods.

Davide Berardi,
Matteo Martelli

Introduction

Who's involved?

Surveillance
Obscuring
Companies
Bad Guys

Programs

Tor

Timing Attack

Astoria

Other ORs and technologies

HORNET

Open Problems

27

Simulazione di Sistemi