

Privacy methods.

Simulazione di Sistemi

September 14, 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

- ▶ Some intelligence organizations obviously do anti-terrorist researches and checks (and that's good!).
- ▶ Some intelligence organizations do that in wrong ways, a normal guy searched "Pressure cooking" and "knap sack" on google and FBI knocked at his house.



Figure: the utah NSA data center "Massive Data Repository", 90k-140k m^2



NSA related 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

According to **Edward Snowden** leaks, the NSA organization has a lot of obscure and top secret projects:

- ▶ PRISM - Software to collect information about every internet communication (US)
 - ▶ Related to some major companies.
- ▶ Tempora - British Intelligence auditing software for internet and phone communications.
- ▶ MonsterMind - **Automated** reaction to attacks.





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

- ▶ PGP - "munitions export without a license".
- ▶ Lavabit - Request to give the public key of the site to the NSA.
- ▶ IP-sec - Snowden leaks revealed that NSA broke (in collaboration with NIST?) the IP-sec suite and his encryption algorithms.
- ▶ Truecrypt - US intelligence failed to decrypt some disks encrypted with truecrypt and fifth amendment protected a suspect.



Let's talk about numbers...

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

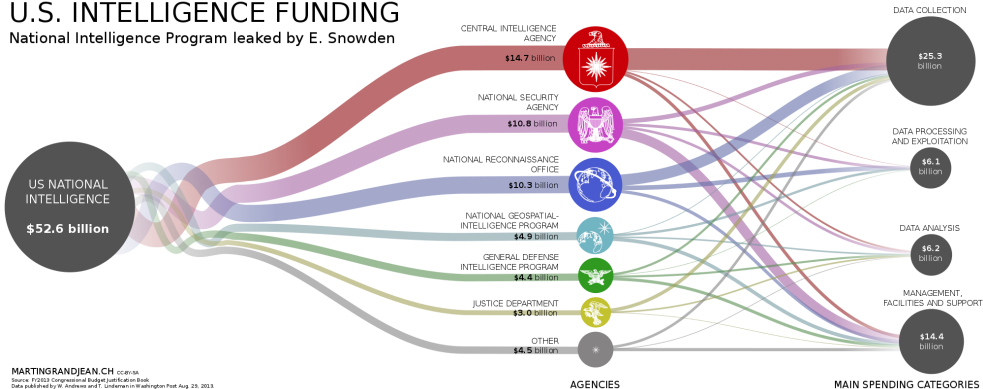
Open Problems

Simulazione di Sistemi

7

U.S. INTELLIGENCE FUNDING

National Intelligence Program leaked by E. Snowden





...and leaks!

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

TOP SECRET//COMINT//REL TO USA, FVEY



User Activity Leads

- Examine settings of phone as well as service providers for geo-location; specific to a certain region
- Networks connected
- Websites visited
- Buddy Lists
- Documents Downloaded
- Encryption used and supported
- User Agents



TOP SECRET//COMINT//REL TO USA, FVEY

12



GEO-Obscuration

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

Some places are sensitive to geo-obscuration (expecially east places like china or japan).

1	Gmail	google.com	gmail.com	Email	English	2014, September (or earlier) to present ^[2]	BLOCKED
1	Google	google.com	google.com	Search	English	2014, May (or earlier) to 2015, July ^[3]	BLOCKED
1	Google Maps	google.com	maps.google.com	Maps	English	2014, May (or earlier) to present ^[4]	BLOCKED
1	Google Docs	google.com	docs.google.com	Sharing	English	2011, May (or earlier) to present ^[5]	BLOCKED
1	Pornhub	pornhub.com	www.pornhub.com	Porn	English	2012, May to present ^[6]	BLOCKED
1	Google Encrypted	google.com	encrypted.google.com	Search	English	2011, March (or earlier) to present ^[7]	BLOCKED
1	Google APIs	google.com	*.googleapis.com	Search	English	2014, September (or earlier) to present ^[8]	BLOCKED
1	Google+	google.com	plus.google.com	Social	English	2011, July to present ^[9]	BLOCKED
1	Google Sites	google.com	sites.google.com	Web Hosting	English	2011, March (or earlier) to present ^[10]	BLOCKED
1	Picasa	google.com	picasaweb.google.com	Sharing	English	2009, July to present ^[11]	BLOCKED
2	Facebook	facebook.com	www.facebook.com	Social	English	2008, July to present	BLOCKED
3	YouTube	youtube.com	www.youtube.com	Sharing	English	2009, March to present ^[12] [13][14][15]	BLOCKED



SOPA and PIPA

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

10

- ▶ Stop Online Piracy Act
- ▶ Gives the control of the obscuration of a site to the proprietary of the copyright (!) and to the government (!!!).
- ▶ In other words...everyone could obscure every site, that use copyrighted contents, from every search engine!
- ▶ Legal penalties and fees to the source of the publication.
- ▶ Incompatible with DMCA, GPL, etc...
- ▶ **Incompatible with VPN, ORs, proxies, etc (!!!).**



Focused ADv

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

11

- ▶ Some companies can do some users profilation.
- ▶ What you've searched, what you say or what you do can be a gold information on who you are and what you're going to do.
- ▶ Maybe the company inform you, and you have nothing to hide, but, you really want to say to a company sensible data?
- ▶ Imagine if a data leakage occurs and someone learns about your google searches...
- ▶ Coff, Coff, Windows 10 keylogger...



Not only powerful adversaries

Privacy methods.

Davide Berardi,
Matteo Martelli

Introduction

Who's involved?

Surveillance
Obscuring
Companies
Bad Guys

12

Programs

Tor

Timing Attack

Astoria

Other ORs and technologies

HORNET

Open Problems

Simulazione di Sistemi

- ▶ Obviously the companies are not the only person interested in our real identity, someone could gain my IP, and/or my geolocation to break into my house when I'm out.
- ▶ So we must ensure our anonymity, just to have a form of security in addition to the classical ones.
- ▶ On the other hand, there is the identity stealing.



Technologies

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

What we can do versus controls?

Can we have some privacy even from the companies/government?

13



Confidentiality and authenticity

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

14

We have a lot of programs to protect our data

- ▶ PGP
- ▶ IPsec
- ▶ OTR-based programs
- ▶ Protonmail  **ProtonMail**
- ▶ TrueCrypt 
- ▶ **Perfect Forward Secrecy**

Some tool for steganography can help but not too much.



Anonymity

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

But for anonymity?

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

15



Anonymous network

Privacy methods.

Davide Berardi,
Matteo Martelli

Introduction

Who's involved?

Surveillance
Obscuring
Companies
Bad Guys

Programs

16

Tor

Timing Attack

Astoria

Other ORs and technologies

HORNET

Open Problems

Simulazione di Sistemi

(mostly) p2p-based networks, no one can identify who put a file on the net.

▶ FreeNet



- ▶ OpenNet mode
- ▶ DarkNet mode

▶ GNUNet



- ▶ Fully Self Contained (like UseNet).
- ▶ Search?
- ▶ Performance?



Mix Networks

Privacy methods.

Davide Berardi,
Matteo Martelli

Introduction

Who's involved?

Surveillance
Obscuring
Companies
Bad Guys

Programs

Tor

Timing Attack

Astoria

Other ORs and
technologies

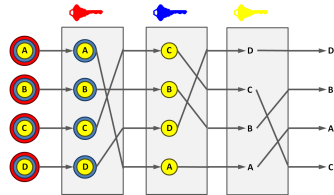
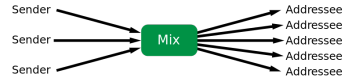
HORNET

Open Problems

Simulazione di Sistemi

17

- ▶ Model of the 1981.
- ▶ Multiple layers of encryption.
- ▶ Select different random nodes to deal with controlled nodes.
- ▶ **Timing attack?**





Old times

Privacy methods.

Davide Berardi,
Matteo Martelli

Introduction

Who's involved?

Surveillance
Obscuring
Companies
Bad Guys

Programs

18

Tor

Timing Attack

Astoria

Other ORs and technologies

HORNET

Open Problems

Simulazione di Sistemi

- ▶ Anonymous remailers: end to end anonymity.
 - ▶ Cypherpunk: remove FROM field and encrypt the mail
 - ▶ Mixmaster: Chain of remailers.
 - ▶ Mixminion: Mixmaster syntax with replies.
 - ▶ nym-server: give a pseudonym to the user detached from his IP.

We'll see that this servers recalls the modern idea of OnionRouting.



Onion Routing

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

The idea of encapsulate cyphered packets in a chain or an "onion".

- ▶ OpenNet? → Hidden services.
- ▶ New possibility like use a proxy to get to the normal internet.

Problems

- ▶ Performance
- ▶ DoS resistance.
- ▶ Mantain links to the users
- ▶ Thrustness of the routers.
- ▶ Confidentiality and autenticity.

19



Onion Routing (2)

Privacy methods.

Davide Berardi,
Matteo Martelli

Introduction

Who's involved?

Surveillance
Obscuring
Companies
Bad Guys

Programs

20

Tor

Timing Attack

Astoria

Other ORs and technologies

HORNET

Open Problems

Simulazione di Sistemi

▶ TOR

▶ We'll come to this later.

▶ i2p

▶ Done for eepsite(s).

▶ Not so much routers/outproxies.

▶ And what for the low latency? → **Timing attacks.**



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

21

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.**



NSA and Tor

Privacy methods.

Davide Berardi,
Matteo Martelli

Introduction

Who's involved?

Surveillance
Obscuring
Companies
Bad Guys

Programs

Tor

22

Timing Attack

Astoria

Other ORs and technologies

HORNET

Open Problems

Simulazione di Sistemi

Tor was made from the naval research labs:

- ▶ Made for the anonymous control and espionage.
- ▶ Tor need a number of exit nodes (and routers) to lead anonymity to an user.
- ▶ if an organization use only his exit nodes it's like to not use them at all.



The Tor revolution

Privacy methods.

Davide Berardi,
Matteo Martelli

Introduction

Who's involved?

Surveillance
Obscuring
Companies
Bad Guys

Programs

Tor

23

Timing Attack

Astoria

Other ORs and technologies

HORNET


Open Problems

Simulazione di Sistemi


Apparently Tor slipped from the hands of the US in the 2004.

- ▶ Russia offered \$114.000 to identify and deface Tor anonymity.
- ▶ NSA now classify TOR as a menace of level *catastrophic*.

TOP SECRET//COMINT//REL TO USA, RUS, CAN, GBR, IND



(U) What is TOR?



- (U) "The Onion Router"
- (U) Enables anonymous internet activity
 - General privacy
 - Non-attribution
 - Circumvention of nation state internet policies
- (U) Hundreds of thousands of users
 - Dissidents (Iran, China, etc)
 - (S//SI//REL) **Terrorists!**
 - (S//SI//REL) Other targets too!

TOP SECRET//COMINT//REL TO USA, RUS, CAN, GBR, IND

But...nobody knows who and what is hidden under the layer of the onion.

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

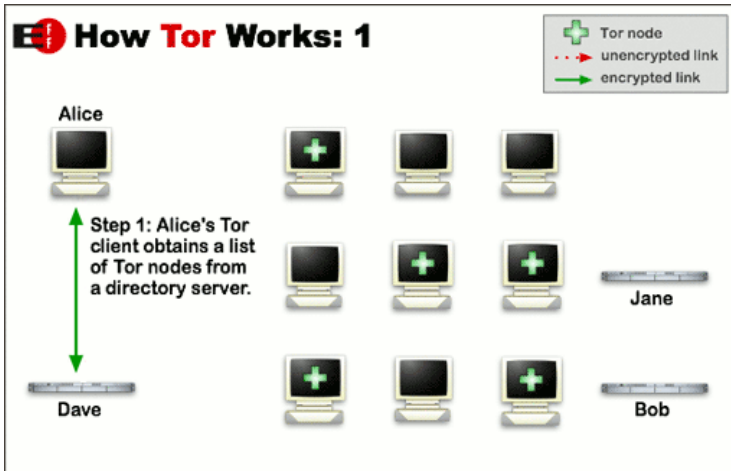
Other ORs and
technologies

HORNET

Open Problems

Simulazione di Sistemi

24





Tor

Tor workings

Privacy methods.

Davide Berardi,
Matteo Martelli

Introduction

Who's involved?

Surveillance
Obscuring
Companies
Bad Guys

Programs

Tor

Timing Attack

Astoria

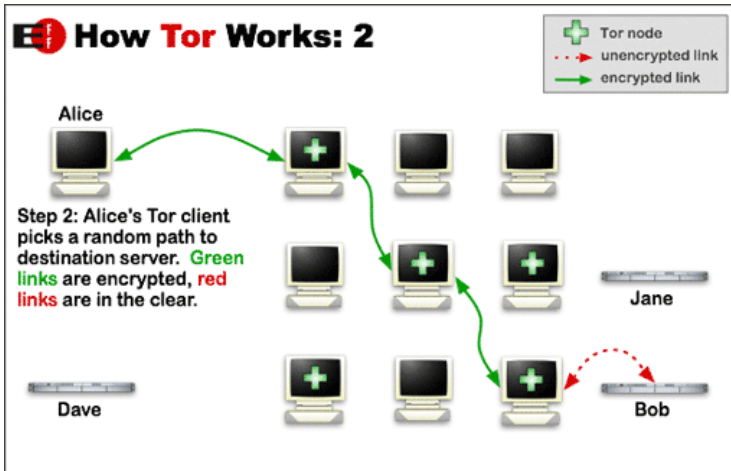
Other ORs and technologies

HORNET

Open Problems

Simulazione di Sistemi

25





Tor

Tor workings

Privacy methods.

Davide Berardi,
Matteo Martelli

Introduction

Who's involved?

Surveillance
Obscuring
Companies
Bad Guys

Programs

Tor

Timing Attack

Astoria

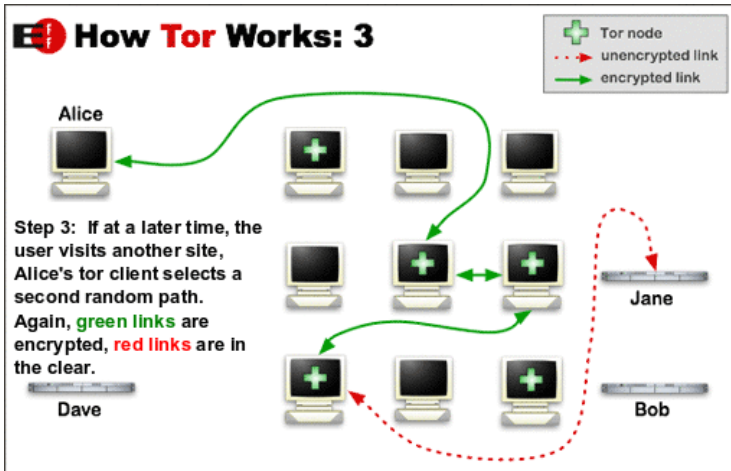
Other ORs and technologies

HORNET

Open Problems

Simulazione di Sistemi

26





Tor

Tor encryption

Privacy methods.

Davide Berardi,
Matteo Martelli

Introduction

Who's involved?

Surveillance
Obscuring
Companies
Bad Guys

Programs

Tor

Timing Attack

Astoria

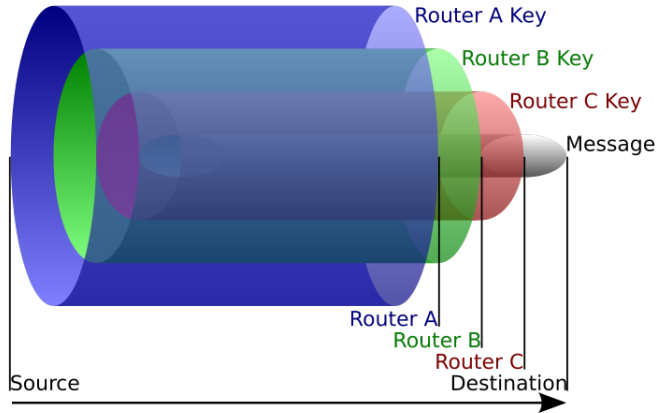
Other ORs and
technologies

HORNET

Open Problems

Simulazione di Sistemi

27





Tor

Tor Hidden Service

Privacy methods.

Davide Berardi,
Matteo Martelli

Introduction

Who's involved?

Surveillance
Obscuring
Companies
Bad Guys

Programs

Tor

Timing Attack

Astoria

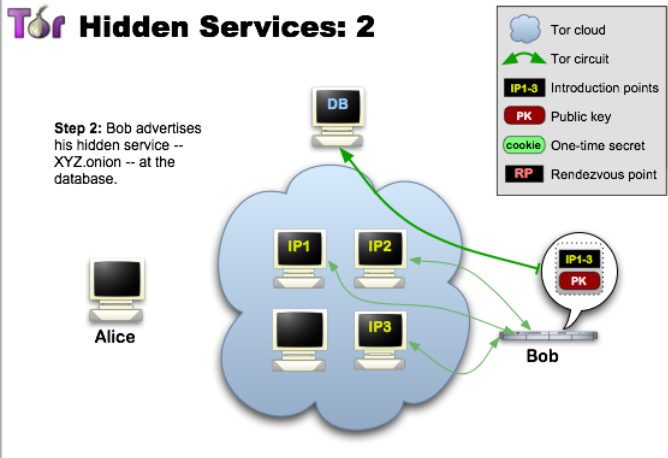
Other ORs and technologies

HORNET

Open Problems

Simulazione di Sistemi

28





Tor

Tor Hidden Service

Privacy methods.

Davide Berardi,
Matteo Martelli

Introduction

Who's involved?

Surveillance

Obscuring

Companies

Bad Guys

Programs

Tor

Timing Attack

Astoria

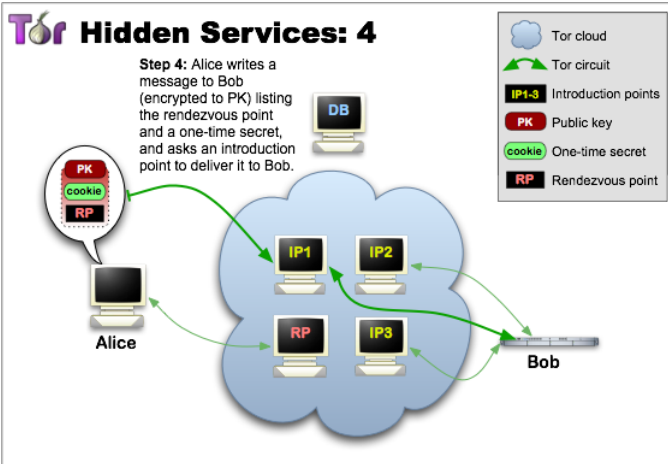
Other ORs and
technologies

HORNET

Open Problems

Simulazione di Sistemi

29





Tor

Tor Hidden Service

Privacy methods.

Davide Berardi,
Matteo Martelli

Introduction

Who's involved?

Surveillance
Obscuring
Companies
Bad Guys

Programs

Tor

Timing Attack

Astoria

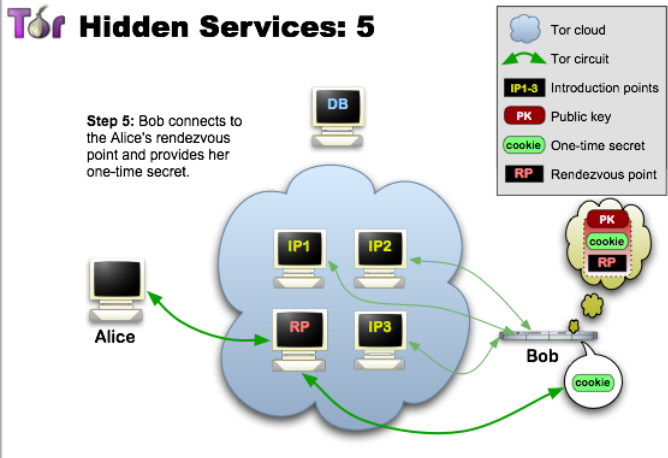
Other ORs and technologies

HORNET

Open Problems

Simulazione di Sistemi

30





Tor

Tor Hidden Service

Privacy methods.

Davide Berardi,
Matteo Martelli

Introduction

Who's involved?

Surveillance
Obscuring
Companies
Bad Guys

Programs

Tor

Timing Attack

Astoria

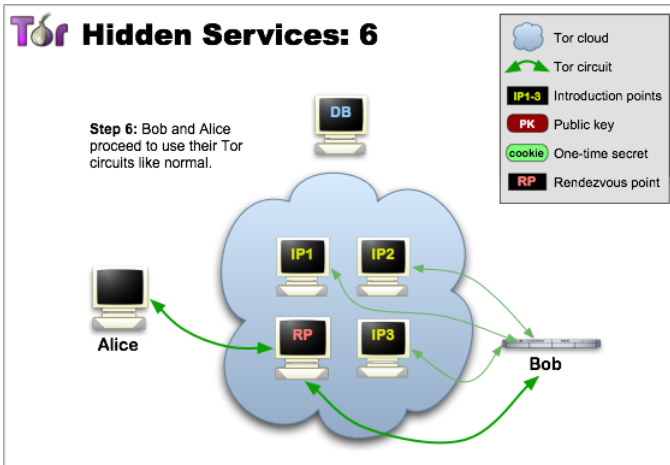
Other ORs and technologies

HORNET

Open Problems

Simulazione di Sistemi

31





Tor

Summary

Privacy methods.

Davide Berardi,
Matteo Martelli

Introduction

Who's involved?

Surveillance
Obscuring
Companies
Bad Guys

Programs

Tor

32

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

33

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

33

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

33

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



- ▶ A file is encrypted with his hash and shared over the network.
- ▶ It can optionally encrypted with the public keys of the dark net users (pseudonym-like) (and signed).
- ▶ The file is so splitted in chunks and shared over the network.
- ▶ Every node can't understand which chunk of which file is processing and what is written in the file itself.



Freenet (2)

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

33

Simulazione di Sistemi



- ▶ The net is guaranteed to resemble a small world network (so the max degree is $\log(n)$) using the Metropolis Hastings algorithm.
- ▶ If a file is not popular and only a chunk is lost, the file is lost forever.