

Privacy methods.

Simulazione di Sistemi

September 15, 2015

Davide Berardi Matteo Martelli
0000712698 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

Possible Solutions

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 interested in laws).



Anonymity

Privacy methods.

Davide Berardi,
Matteo Martelli

Introduction

2

Who's involved?

Surveillance
Obscuring
Companies
Bad Guys

Programs

Tor

Timing Attack

Astoria

Possible Solutions

We will talk about anonymity as the property of disconnect the user of a service from some basic properties:

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

Sometimes we need to re-associate 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

Possible Solutions

"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

Possible Solutions

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

Possible Solutions

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?

6

Surveillance

Obscuring

Companies

Bad Guys

Programs

Tor

Timing Attack

Astoria

Possible Solutions

- ▶ 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

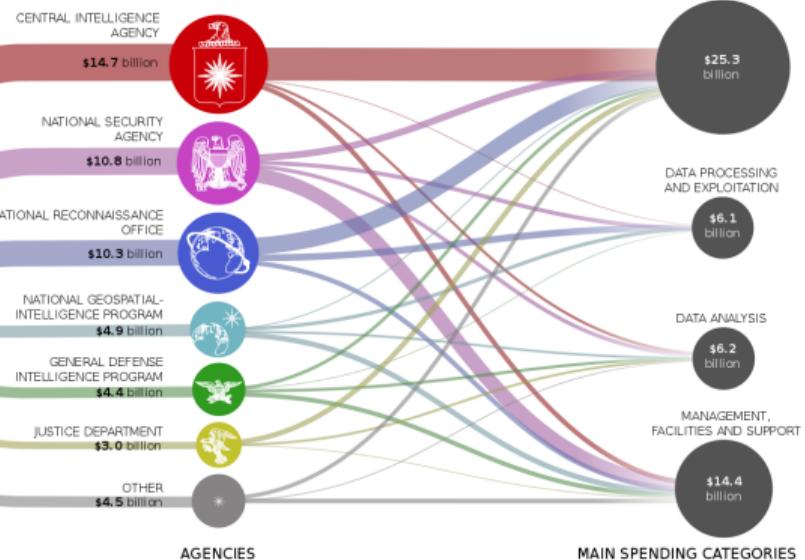
Possible Solutions

U.S. INTELLIGENCE FUNDING

National Intelligence Program leaked by E. Snowden

7

US NATIONAL
INTELLIGENCE
\$52.6 billion



MARTINGRANDJEAN.CH ccavas
Source: FY2013 Congressional Budget Justification Book
Data published by W. Andrews and T. Underman in Washington Post Aug. 29, 2013.



...and leaks!

Privacy methods.

Davide Berardi,
Matteo Martelli

Introduction

Who's involved?

Surveillance

Obscuring

Companies

Bad Guys

Programs

Tor

Timing Attack

Astoria

Possible Solutions

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

Possible Solutions

Simulazione di Sistemi

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

#	Domain	Original URL	Obscured URL	Type	Language	Last Update	Status
1	Omail	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	2005, 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

Possible Solutions

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

Possible Solutions

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

Programs

Tor

Timing Attack

Astoria

Possible Solutions

12

- ▶ 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

13

What we can do versus controls?

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

Tor

Timing Attack

Astoria

Possible Solutions

Simulazione di Sistemi



Confidentiality and authenticity

Privacy methods.

Davide Berardi,
Matteo Martelli

Introduction

Who's involved?

Surveillance
Obscuring
Companies
Bad Guys

Programs

14

Tor

Timing Attack

Astoria

Possible Solutions

Simulazione di Sistemi

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

15

Tor

Timing Attack

Astoria

Possible Solutions

But for anonymity?

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



Anonymous network

Privacy methods.

Davide Berardi,
Matteo Martelli

Introduction

Who's involved?

Surveillance

Obscuring

Companies

Bad Guys

Programs

16

Tor

Timing Attack

Astoria

Possible Solutions

(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

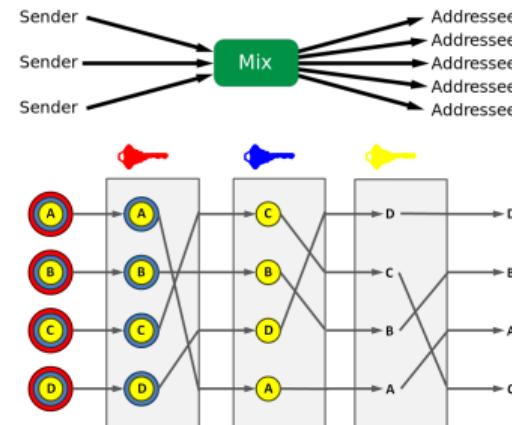
Timing Attack

Astoria

Possible Solutions

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

Possible Solutions

- ▶ 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

19

Tor

Timing Attack

Astoria

Possible Solutions

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.



Onion Routing (2)

Privacy methods.

Davide Berardi,
Matteo Martelli

Introduction

Who's involved?

Surveillance
Obscuring
Companies
Bad Guys

Programs

20

Tor

Timing Attack

Astoria

Possible Solutions

- ▶ 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.**



NSA and Tor

Privacy methods.

Davide Berardi,
Matteo Martelli

Introduction

Who's involved?

Surveillance
Obscuring
Companies
Bad Guys

Programs

Tor

21

Timing Attack

Astoria

Possible Solutions

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

22

Timing Attack

Astoria

Possible Solutions

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*.

(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!

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

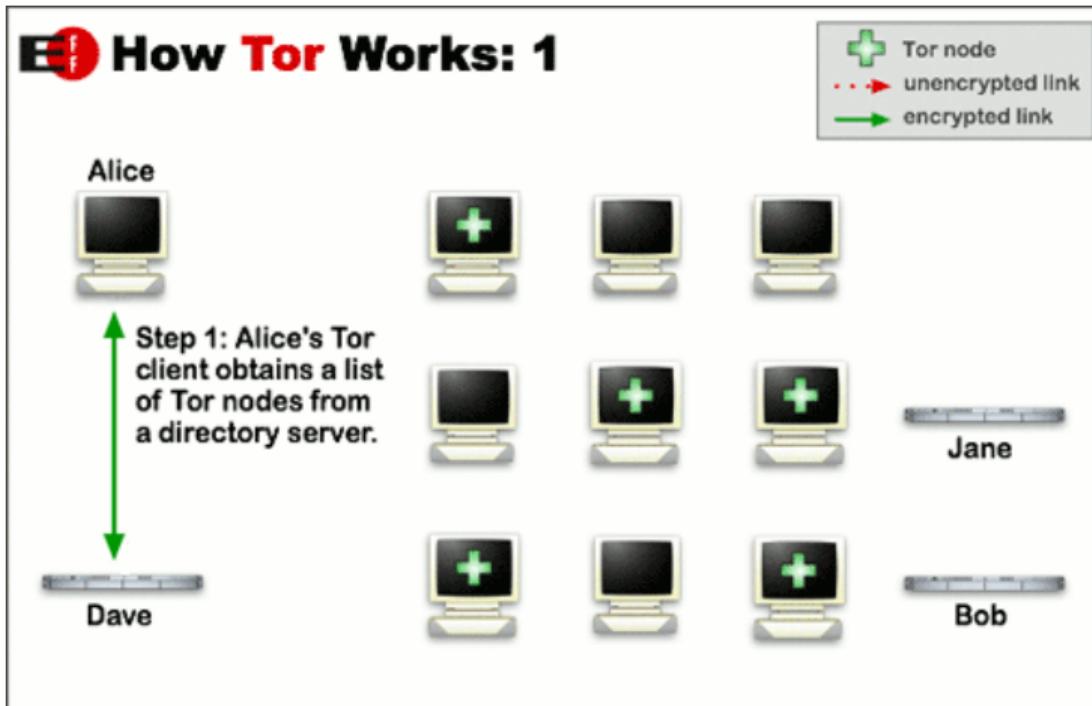
23

Timing Attack

Astoria

Possible Solutions

Simulazione di Sistemi





Tor

Tor workings

Privacy methods.

Davide Berardi,
Matteo Martelli

Introduction

Who's involved?

Surveillance
Obscuring
Companies
Bad Guys

Programs

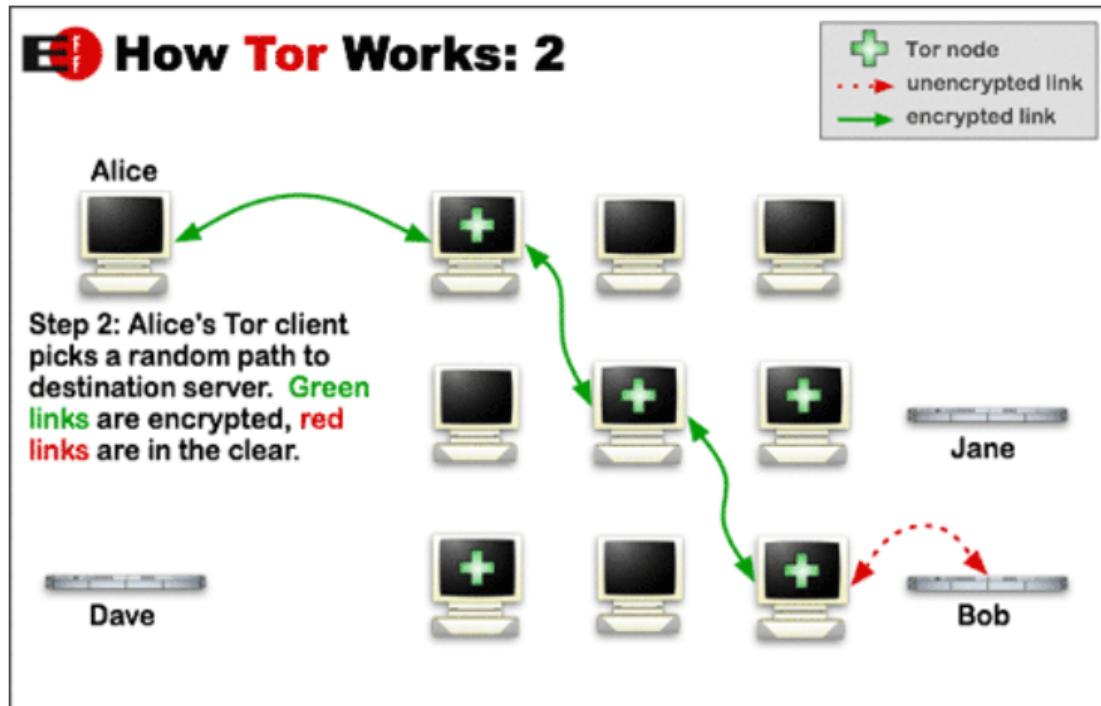
Tor

Timing Attack

Astoria

Possible Solutions

24





Tor

Tor workings

Privacy methods.

Davide Berardi,
Matteo Martelli

Introduction

Who's involved?

Surveillance
Obscuring
Companies
Bad Guys

Programs

Tor

25

Timing Attack

Astoria

Possible Solutions

E How Tor Works: 3

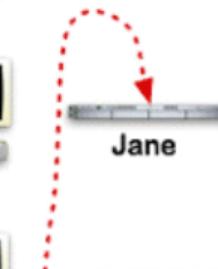
+ Tor node
- -> unencrypted link
-> encrypted link

Alice



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.

Dave



Jane

Bob



Tor

Tor encryption

Privacy methods.

Davide Berardi,
Matteo Martelli

Introduction

Who's involved?

Surveillance
Obscuring
Companies
Bad Guys

Programs

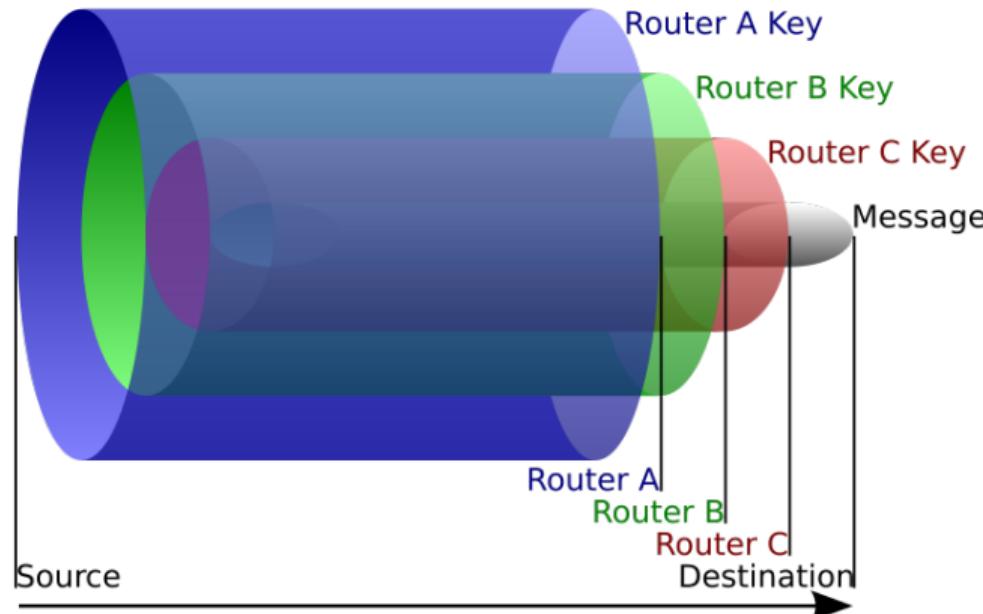
Tor

26

Timing Attack

Astoria

Possible Solutions





Tor

Tor Hidden Service

Privacy methods.

Davide Berardi,
Matteo Martelli

Introduction

Who's involved?

Surveillance
Obscuring
Companies
Bad Guys

Programs

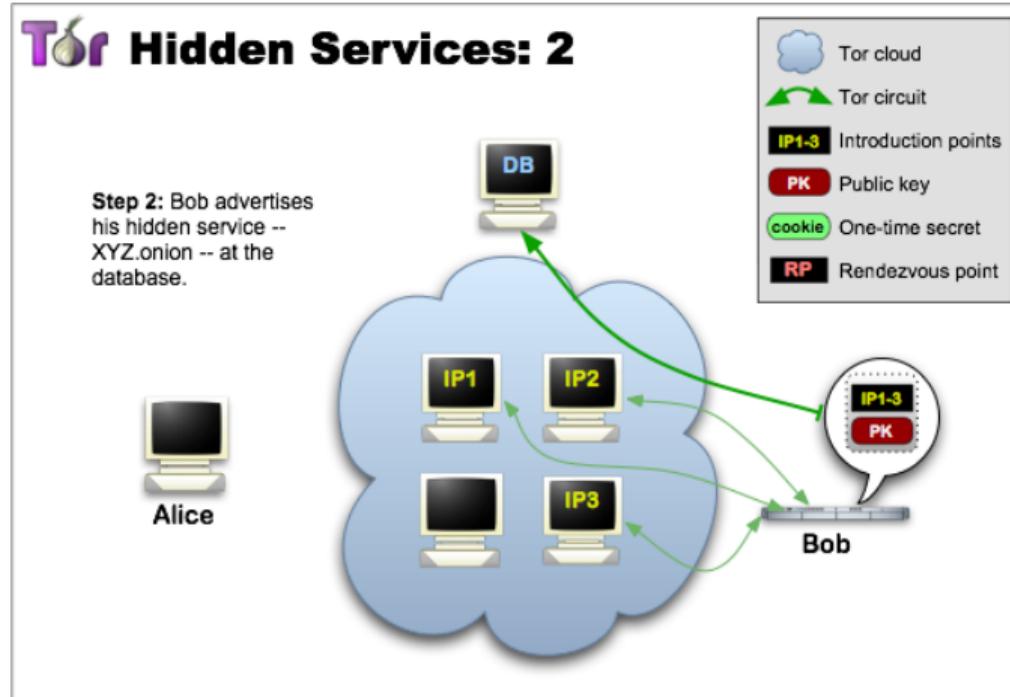
Tor

Timing Attack

Astoria

Possible Solutions

27





Tor

Tor Hidden Service

Privacy methods.

Davide Berardi,
Matteo Martelli

Introduction

Who's involved?

Surveillance
Obscuring
Companies
Bad Guys

Programs

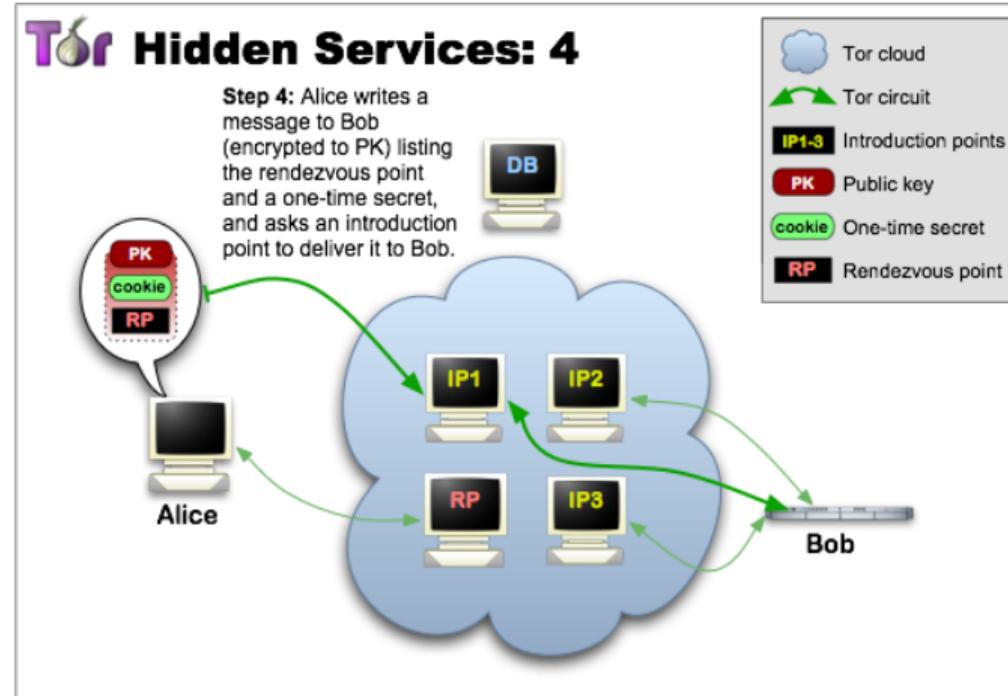
Tor

Timing Attack

Astoria

Possible Solutions

28





Tor

Tor Hidden Service

Privacy methods.

Davide Berardi,
Matteo Martelli

Introduction

Who's involved?

Surveillance
Obscuring
Companies
Bad Guys

Programs

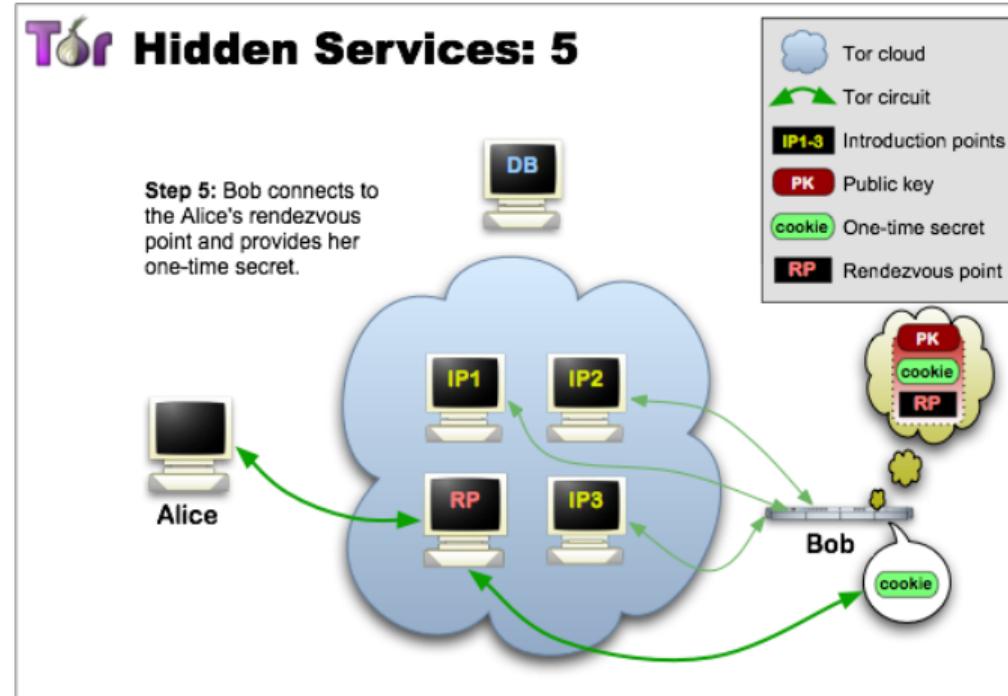
Tor

Timing Attack

Astoria

Possible Solutions

29





Tor

Tor Hidden Service

Privacy methods.

Davide Berardi,
Matteo Martelli

Introduction

Who's involved?

Surveillance
Obscuring
Companies
Bad Guys

Programs

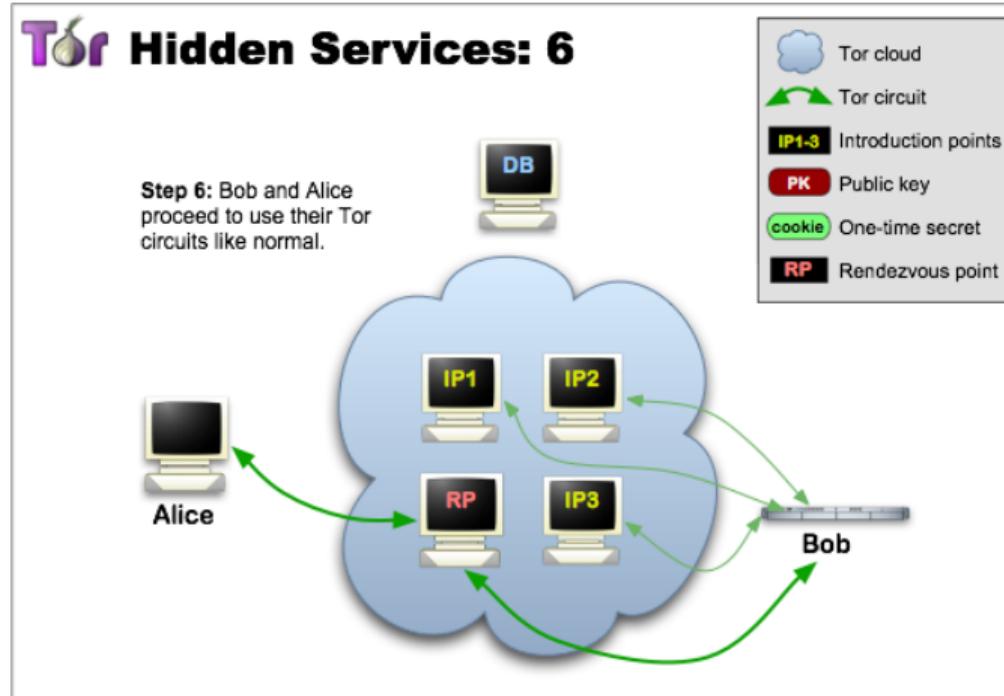
Tor

Timing Attack

Astoria

Possible Solutions

30





Tor

Summary

Privacy methods.

Davide Berardi,
Matteo Martelli

Introduction

Who's involved?

Surveillance
Obscuring
Companies
Bad Guys

Programs

Tor

31

Timing Attack

Astoria

Possible Solutions

- ▶ 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

32

Astoria

Possible Solutions

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.)



Timing analysis based attacks

Privacy methods.

Davide Berardi,
Matteo Martelli

Introduction

Who's involved?

Surveillance

Obscuring

Companies

Bad Guys

Programs

Tor

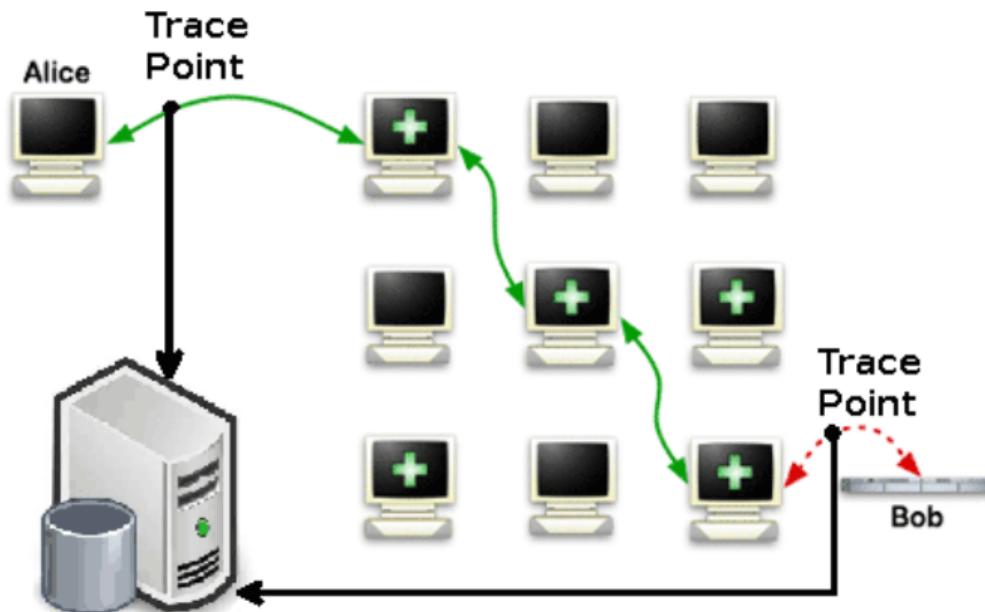
Timing Attack

33

Astoria

Possible Solutions

Simulazione di Sistemi





Why simulation?

Privacy methods.

Davide Berardi,
Matteo Martelli

Introduction

Who's involved?

Surveillance

Obscuring
Companies
Bad Guys

Programs

Tor

Timing Attack

34

Astoria

Possible Solutions

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 about the timing attack feasibility and estimate the number of resources needed by an attacker.**



Simulation results

Privacy methods.

Davide Berardi,
Matteo Martelli

Introduction

Who's involved?

Surveillance

Obscuring

Companies

Bad Guys

Programs

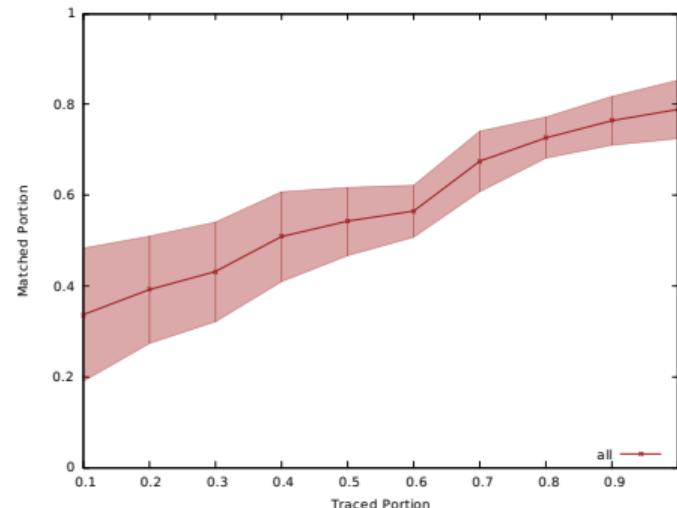
Tor

Timing Attack

35

Astoria

Possible Solutions



Tracing **half** of the Tor network, an attacker may be able to understand the relationships between the nodes of a **quarter** of the Tor network.



Simulation results

Privacy methods.

Davide Berardi,
Matteo Martelli

Introduction

Who's involved?

Surveillance

Obscuring

Companies

Bad Guys

Programs

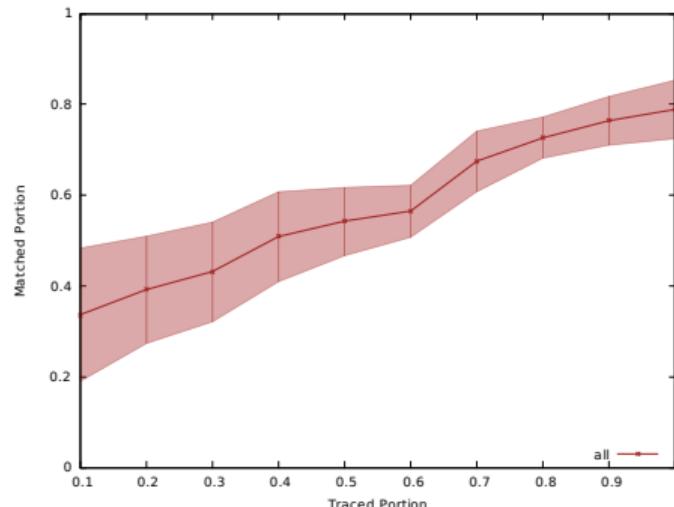
Tor

Timing Attack

36

Astoria

Possible Solutions



- ▶ Timing attack is **feasible**.
- ▶ It requires a **LOT** of resources.



Too much?

Privacy methods.

Davide Berardi,
Matteo Martelli

Introduction

Who's involved?

Surveillance
Obscuring
Companies
Bad Guys

Programs

Tor

Timing Attack

37

Astoria

Possible Solutions

Who can face such big amount of resources?





NSA timing attack on clients

NSA slides leak

Privacy methods.

Davide Berardi,
Matteo Martelli

Introduction

Who's involved?

Surveillance
Obscuring
Companies
Bad Guys

Programs

Tor

Timing Attack

38

Astoria

Possible Solutions

Simulazione di Sistemi

TOP SECRET//COMINT// REL FVEY

(TS//SI)

Technical Analysis: Timing Pattern

Send packets back to the client that are detectable by passive accesses to find client IPs for Tor users.

- Current: GCHQ has research paper and demonstrated capability in the lab.
- Goal: Can we expand to other owned nodes?



NSA timing attack on servers

NSA slides leak

Privacy methods.

Davide Berardi,
Matteo Martelli

Introduction

Who's involved?

Surveillance

Obscuring

Companies

Bad Guys

Programs

Tor

Timing Attack

(39)

Astoria

Possible Solutions

TOP SECRET//COMINT// REL FVEY

Exploitation: Web Server Enabling

(TS//SI)

Given CNE access to web server modify the server to enable a “timing/counting” attack similar to timing pattern idea.

- Current: GCHQ has a research paper and demonstrated the technique in the lab.



Measuring AS-level adversaries against Tor

Privacy methods.

Davide Berardi,
Matteo Martelli

Introduction

Who's involved?

Surveillance
Obscuring
Companies
Bad Guys

Programs

Tor

Timing Attack

Astoria

40

Possible Solutions

- ▶ Multiple Autonomous Systems (AS) collude with each other performing time based attacks and collecting asymmetric data.
- ▶ Up to 40% of circuits constructed by the current Tor client are vulnerable to AS-level attackers.
- ▶ Connections from China were found to be most vulnerable to AS-level attackers with up to 86% of all Tor circuits.



Mitigating AS-level adversaries against Tor

ASes correlations

Privacy methods.

Davide Berardi,
Matteo Martelli

Introduction

Who's involved?

Surveillance
Obscuring
Companies
Bad Guys

Programs

Tor

Timing Attack

Astoria

41

Possible Solutions

Connections between ASes are negotiated as business arrangements.

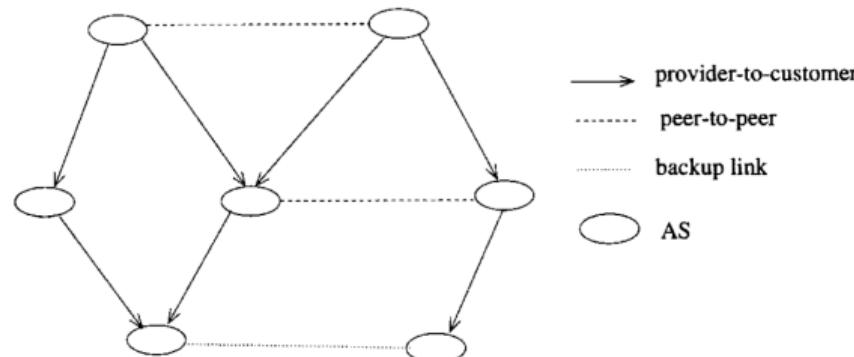


Fig. 3. Hierarchical AS interconnection.

The idea

Building a graph of ASes correlations to identify vulnerable paths.



Astoria

Privacy methods.

Davide Berardi,
Matteo Martelli

Introduction

Who's involved?

Surveillance

Obscuring

Companies

Bad Guys

Programs

Tor

Timing Attack

Astoria

42

Possible Solutions

- ▶ Use of path prediction to avoid Tor vulnerable paths.
i.e. The entry node and the exit node may be selected together if their ASes are unrelated to each others.
- ▶ Able to perform load-balancing at least as well as the vanilla Tor client.



Possible Solutions

Privacy methods.

Davide Berardi,
Matteo Martelli

Introduction

Who's involved?

Surveillance

Obscuring

Companies

Bad Guys

Programs

Tor

Timing Attack

Astoria

Possible Solutions

43



"I deplore the lack of internet privacy
and so do my 5,000 Facebook friends!"





Possible Solutions

Privacy methods.

Davide Berardi,
Matteo Martelli

Introduction

Who's involved?

Surveillance
Obscuring
Companies
Bad Guys

Programs

Tor

Timing Attack

Astoria

Possible Solutions

44

- ▶ Need of privacy rules reinforcement and more investments on network security solutions
 - (i.e. In April 2014, the European Court of Justice declared invalid the EU Data Retention Directive.)¹
- ▶ Academic researches
- ▶ FOSS

¹According to the directive, member states will have to store citizens' telecommunications data for a minimum of 6 months and at most 24 months. Under the directive the police and security agencies will be able to request access to details such as IP address and time of use of every email, phone call and text message sent or received.

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

Possible Solutions

44

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

Now the shared key $K = k_b^a = k_a^b = \alpha^{ab} \text{mod } p$ is known to Alice and Bob².

²For the little Fermat theorem ($a^p \equiv a \text{ mod } p$) 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

Possible Solutions (44)

- ▶ 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

Privacy methods.

Davide Berardi,
Matteo Martelli

Introduction

Who's involved?

Surveillance
Obscuring
Companies
Bad Guys

Programs

Tor

Timing Attack

Astoria

Possible Solutions

44



- ▶ A file is encrypted with his hash and shared over the network.
- ▶ It can optionally be 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

Possible Solutions (44)



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



Tor Attacks

Privacy methods.

Davide Berardi,
Matteo Martelli

Introduction

Who's involved?

Surveillance

Obscuring

Companies

Bad Guys

Programs

Tor

Timing Attack

Astoria

Possible Solutions

(44)

- ▶ Sylpheed
- ▶ Bad Apple
- ▶ Sniper
- ▶ Heartbleed
- ▶ Bundle attacks
- ▶ Protocol attacks
- ▶ ...users...



AS map

Privacy methods.

Davide Berardi,
Matteo Martelli

Introduction

Who's involved?

Surveillance
Obscuring
Companies
Bad Guys

Programs

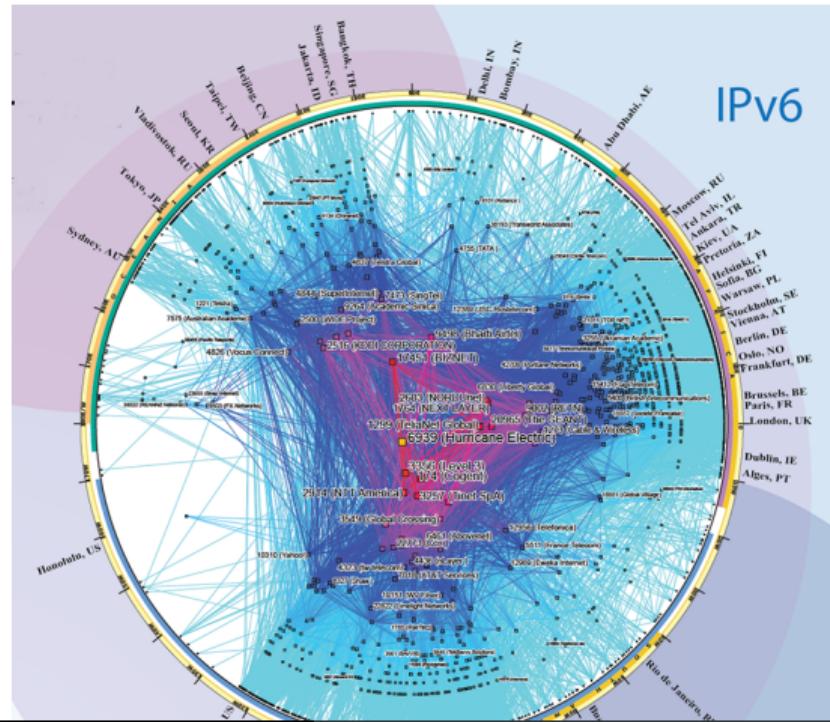
Tor

Timing Attack

Astoria

Possible Solutions

45





Bibliography I

Privacy methods.

Davide Berardi,
Matteo Martelli

Introduction

Who's involved?

Surveillance

Obscuring
Companies
Bad Guys

Programs

Tor

Timing Attack

Astoria

Possible Solutions

46

- [Abe99] Masayuki Abe, *Mix-networks on permutation networks*, Advances in cryptology-ASIACRYPT'99, Springer, 1999, pp. 258–273.
- [Ack13] Spencer Ackerman, *Lavabit email service abruptly shut down citing government interference*, The Guardian 9 (2013).
- [Art13] C Arthur, *Nsa scandal: what data is being monitored and how does it work*, The Guardian (2013).
- [BGH⁺] K Bennett, C Grothoff, T Horozov, I Patrascu, and T Stef, *Gnunet-a truly anonymous networking infrastructure. maggio 2002*.
- [CSWH01] Ian Clarke, Oskar Sandberg, Brandon Wiley, and Theodore W Hong, *Freenet: A distributed anonymous information storage and retrieval system*, Designing Privacy Enhancing Technologies, Springer, 2001, pp. 46–66.
- [DH03] Naganand Doraswamy and Dan Harkins, *Ipsec: the new security standard for the internet, intranets, and virtual private networks*, Prentice Hall Professional, 2003.
- [DMS04] Roger Dingledine, Nick Mathewson, and Paul Syverson, *Tor: The second-generation onion router*, Tech. report, DTIC Document, 2004.



Bibliography II

Privacy methods.

Davide Berardi,
Matteo Martelli

Introduction

Who's involved?

Surveillance

Obscuring

Companies

Bad Guys

Programs

Tor

Timing Attack

Astoria

Possible Solutions

47

- [Dra14] Sylvain Drapau, *Protonmail, client mail crypté développé par le cern.*
- [ES09] Matthew Edman and Paul Syverson, *As-awareness in tor path selection*, Proceedings of the 16th ACM conference on Computer and communications security, ACM, 2009, pp. 380–389.
- [GMP13] Glenn Greenwald, Ewen MacAskill, and Laura Poitras, *Edward Snowden: the whistleblower behind the nsa surveillance revelations*, The Guardian 9 (2013).
- [GRS99] David Goldschlag, Michael Reed, and Paul Syverson, *Onion routing*, Communications of the ACM 42 (1999), no. 2, 39–41.
- [Sal10] Juha Salo, *Recent attacks on tor*, Aalto University (2010).
- [Sch13] Bruce Schneier, *Attacking tor: how the nsa targets users' online anonymity*, The Guardian 4 (2013).
- [SNZ⁺15] Oleksii Starov, Rishab Nithyanand, Adva Zair, Phillipa Gill, and Michael Schapira, *Measuring and mitigating as-level adversaries against tor*, arXiv preprint arXiv:1505.05173 (2015).
- [Spo13] Politics Opinions Local Sports, *Nsa slides explain the prism data-collection program.*
- [tora] *Tor anonymizer network among nsa's targets, snowden leaks reveal.*



Bibliography III

Privacy methods.

Davide Berardi,
Matteo Martelli

Introduction

Who's involved?

Surveillance

Obscuring

Companies

Bad Guys

Programs

Tor

Timing Attack

Astoria

Possible Solutions

48

- [torb] *Tor manual*, <https://www.torproject.org/docs/tor-manual-dev.html.en>.
- [torc] *Tor: Overview*, <https://www.torproject.org/about/overview.html.en>.
- [vRV] Nicky van Rijnsbergen and Kevin Valk, *Tor vs the nsa*.
- [ZH11] Bassam Zantout and Ramzi Haraty, *I2p data communication system*, Proceedings of the tenth international conference on networks, 2011, pp. 401–409.
- [Zim95] Philip R Zimmermann, *The official pgp user's guide*, MIT press, 1995.