NEXTLEAP

https://nextleap.eu/

ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

Anonymous communications

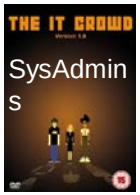
(a crash course in 7 minutes)

CPDP -
24th January 2018

Carmela Troncoso
carmela.troncoso@epfl.ch

Privacy in electronic communications

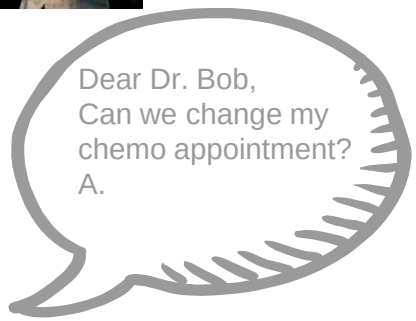
Intelligence agencies



The Boss

Anybody curious

ISPs

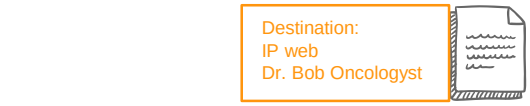


Alice

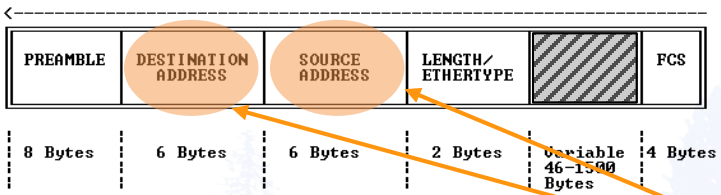
Bob

A Network

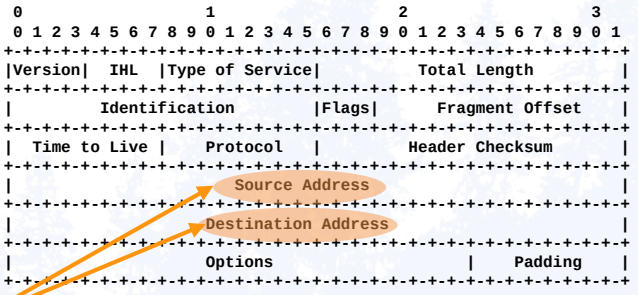
But we can encrypt! What is the problem?



A Network



Ethernet
(IEEE 802.3, 1997)

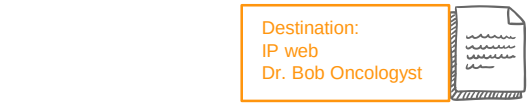


IPv4 Header
(RFC 791, 1981)

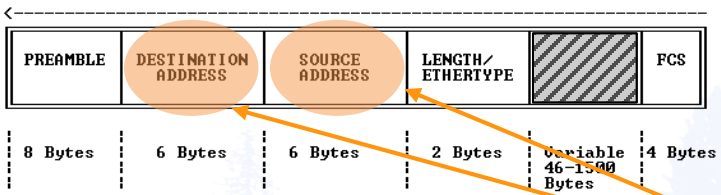
Weak identifier

Same for TCP, SMTP, IRC, HTTP, ...

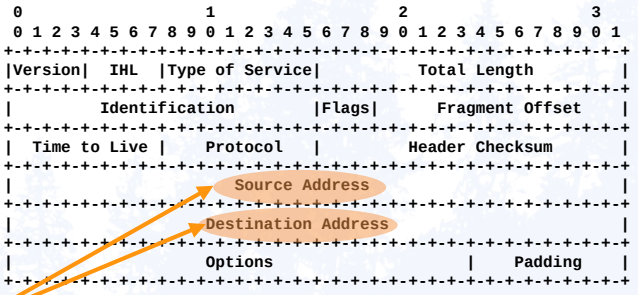
The problem is **Traffic Analysis**!!



A Network



Ethernet
(IEEE 802.3, 1997)



IPv4 Header
(RFC 791, 1981)

Weak identifier

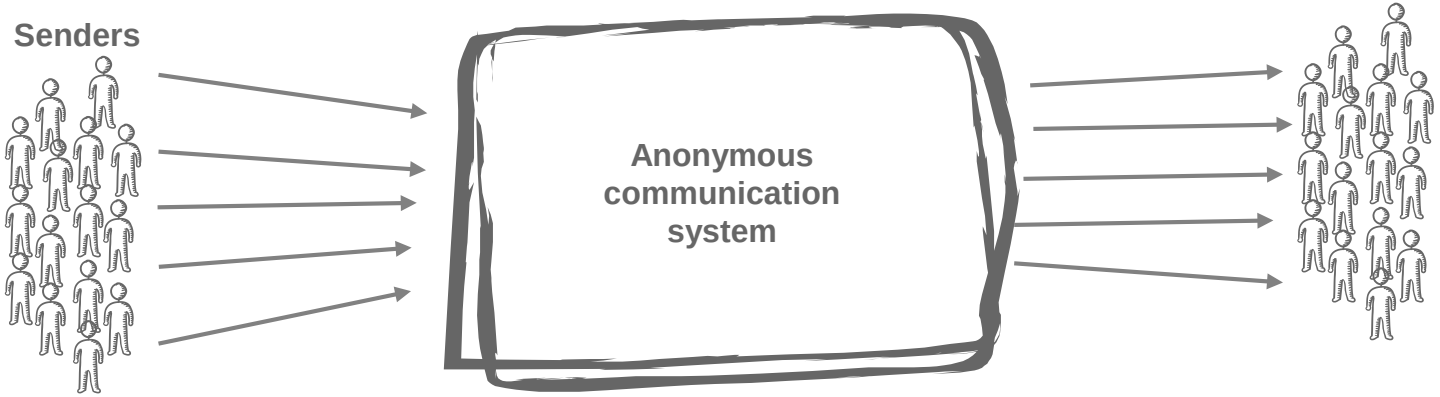
Same for TCP, SMTP, IRC, HTTP, ...

The solution: anonymous communications

IDs
Timing
Volume
Length
...

- **Receivers**

- **Senders**



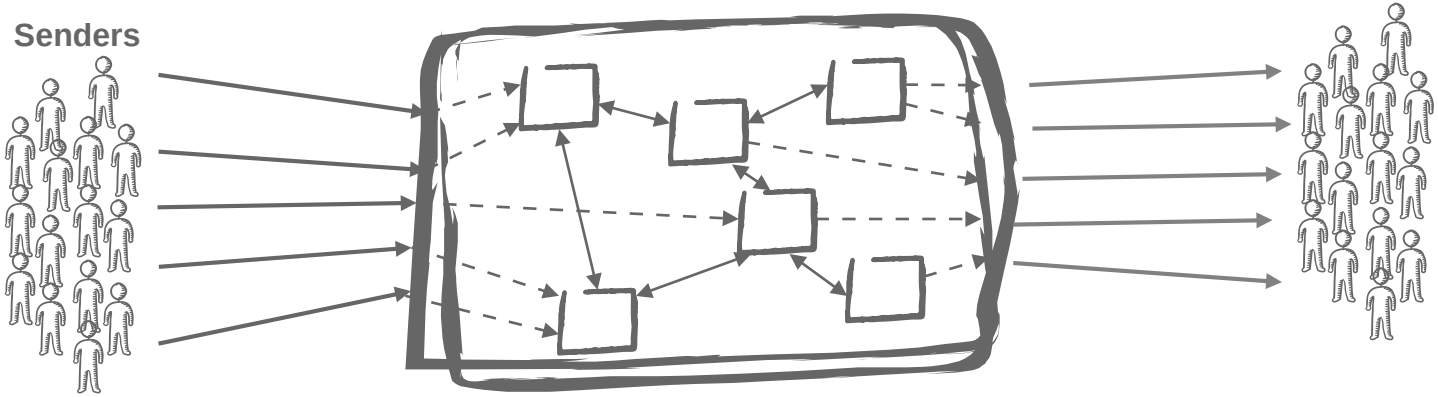
- **Bitwise unlinkability**
  - Crypto to make inputs and outputs bit patterns different

- **(re)packetizing + (re)schedule**
  - Destroy patterns (traffic analysis resistance)

The solution: anonymous communications

IDs
Timing
Volume
Length
...

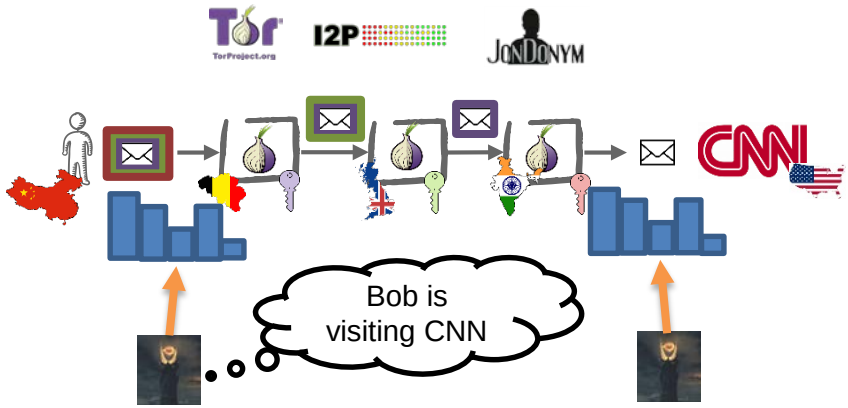
- **Receivers**
- **Senders**



- **Bitwise unlinkability**
  - Crypto to make inputs and outputs bit patterns different
- **(re)packetizing + (re)schedule + (re)routing,**
  - Destroy patterns (traffic analysis resistance)
  - Load balancing
  - Distribute trust

Anonymous communications out there

Low Latency

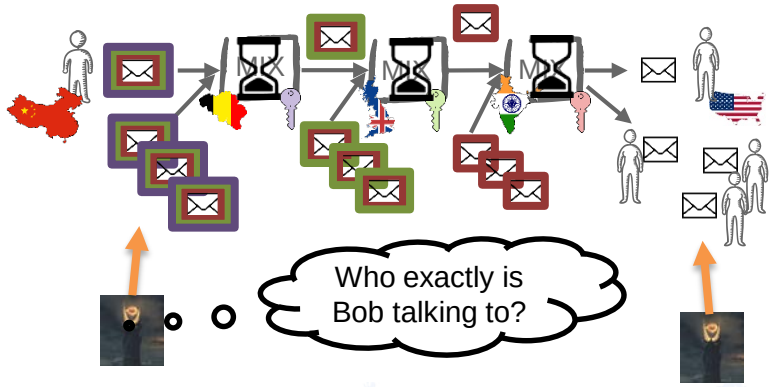


Cannot resist Global Adversary
(assumes adversary cannot see
both edges)

Web browsing, Instant Messaging, streaming

High Latency

MIXMASTER / MIXMINION



Global Adversary resistance
at the cost of latency
(and long term patterns revealed)

Email, Voting

Panoramix

THE BEST OF BOTH WORLDS

Lots of challenges ahead!

Deploying new things or work on deployed ones

– finding volunteers and diversity is a hassle

Modeling adversaries

– we don’t know what the bad guys know

Measure anonymity

– what is anonymity? when is it enough?