The Parrot is Dead: Observing Unobservable Network Communications

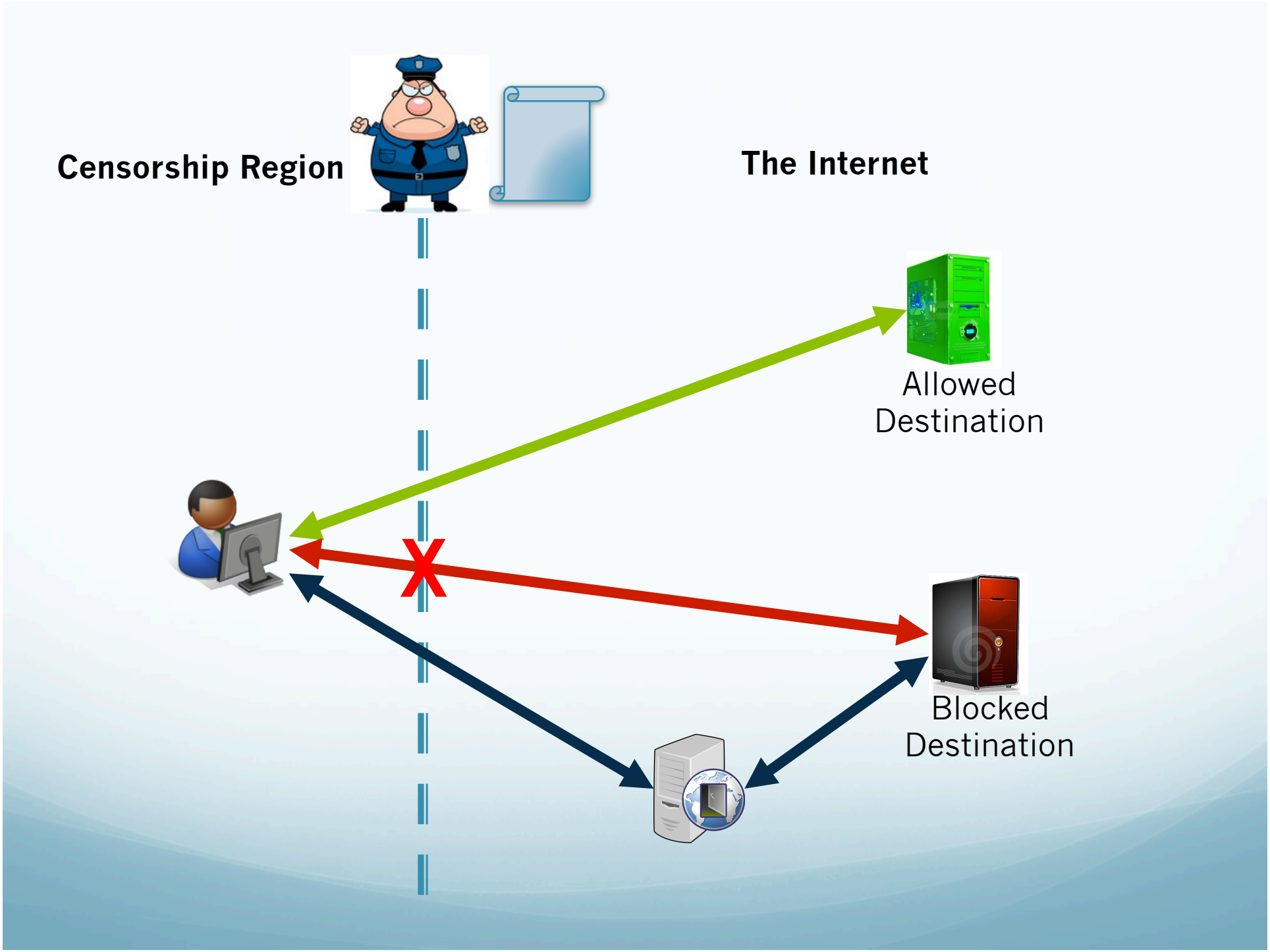
Amir Houmansadr Chad Brubaker Vitaly Shmatikov

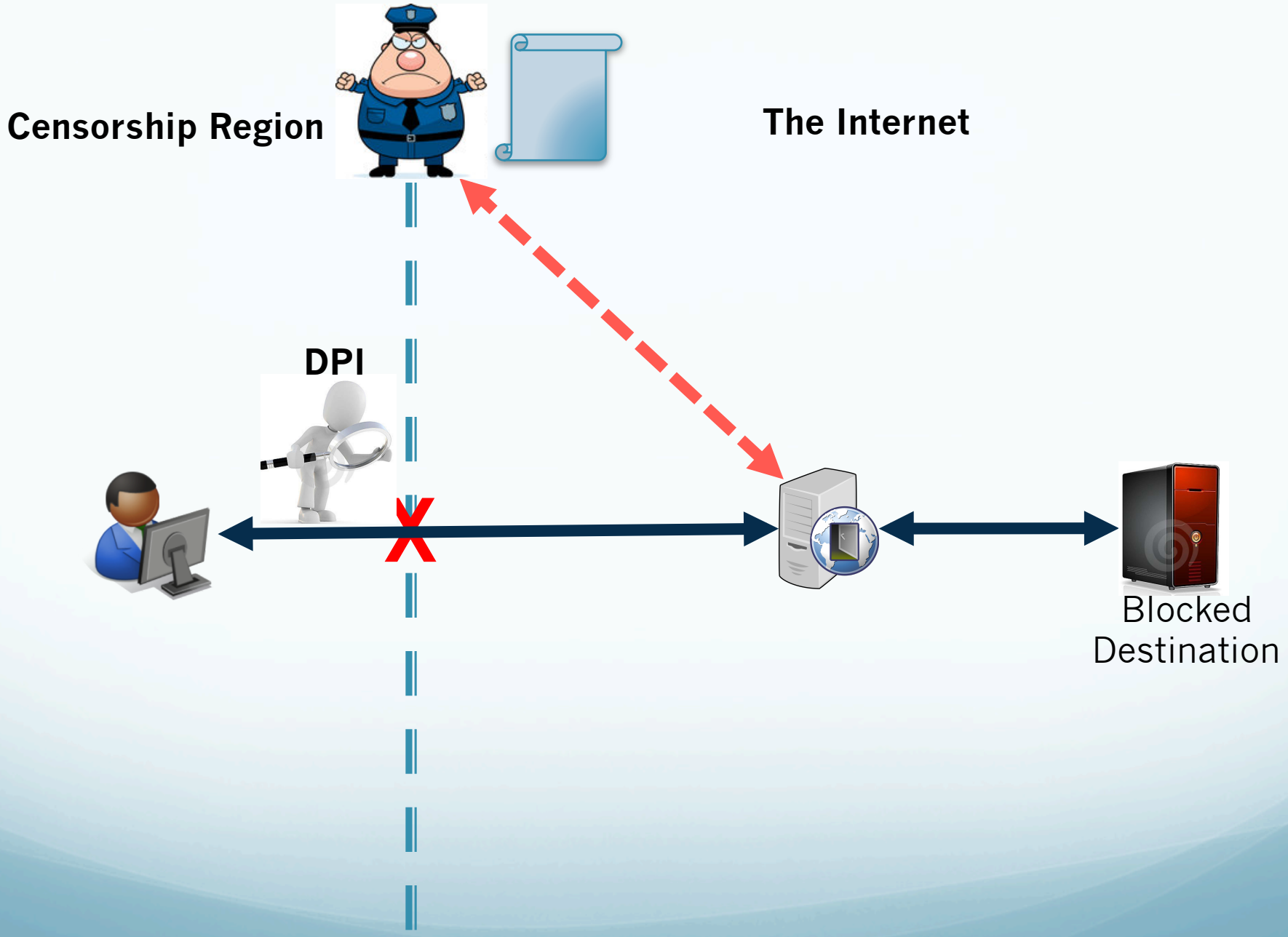
THE UNIVERSITY OF TEXAS AT AUSTIN

Internet Censorship

- The Internet is a big **threat** to repressive regimes!
- Repressive regimes **censor** the Internet:
  - IP filtering, DNS hijacking, Deep packet-inspection, etc.
- Circumvention systems

Anonymizer®

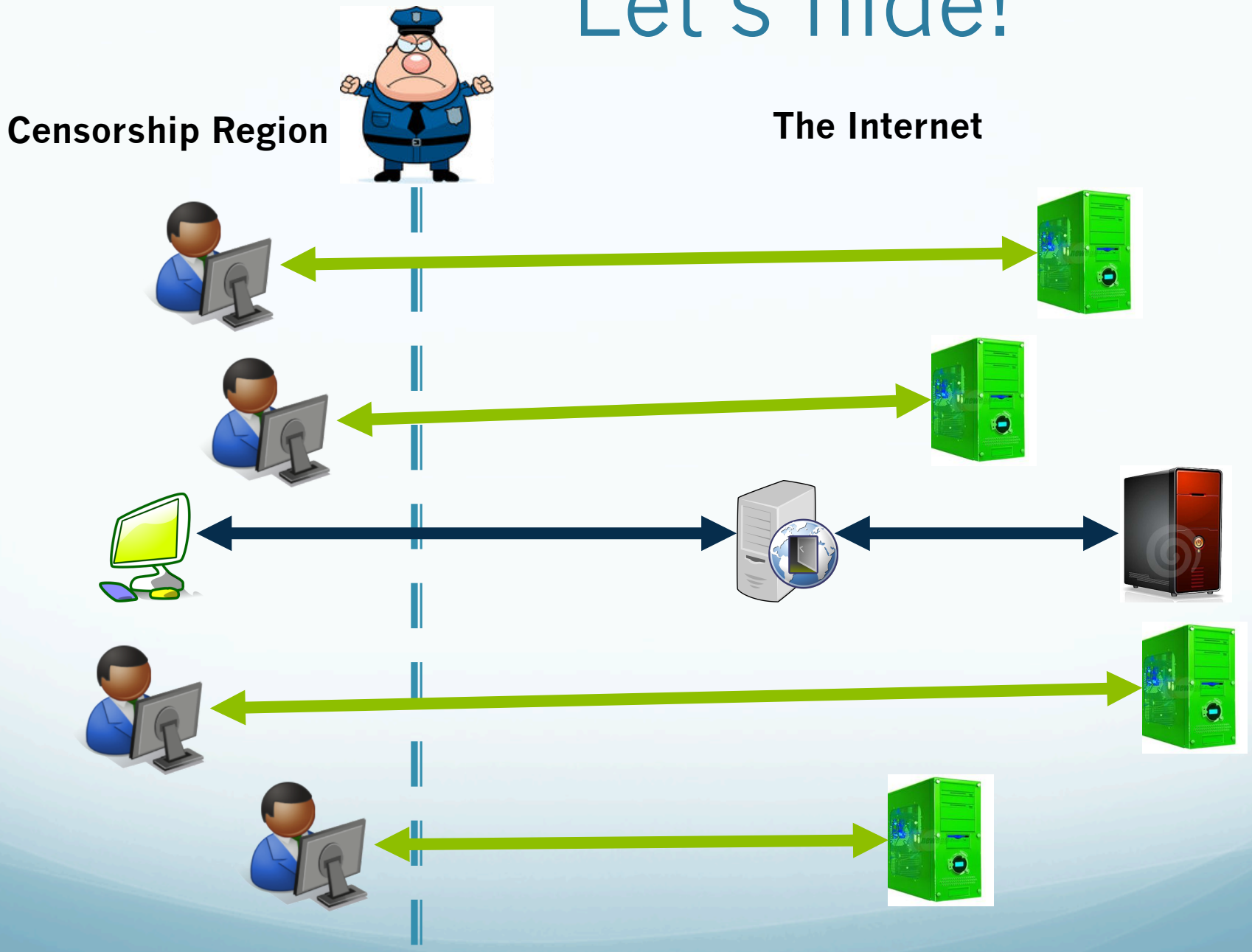

Censorship Region
The Internet
Allowed Destination
Blocked Destination


Censorship Region
The Internet
DPI
Blocked
Destination

We need **unobservable circumvention**

Censors should not be able to identify circumvention traffic or end-hosts through passive, active, or proactive techniques

Let's hide!

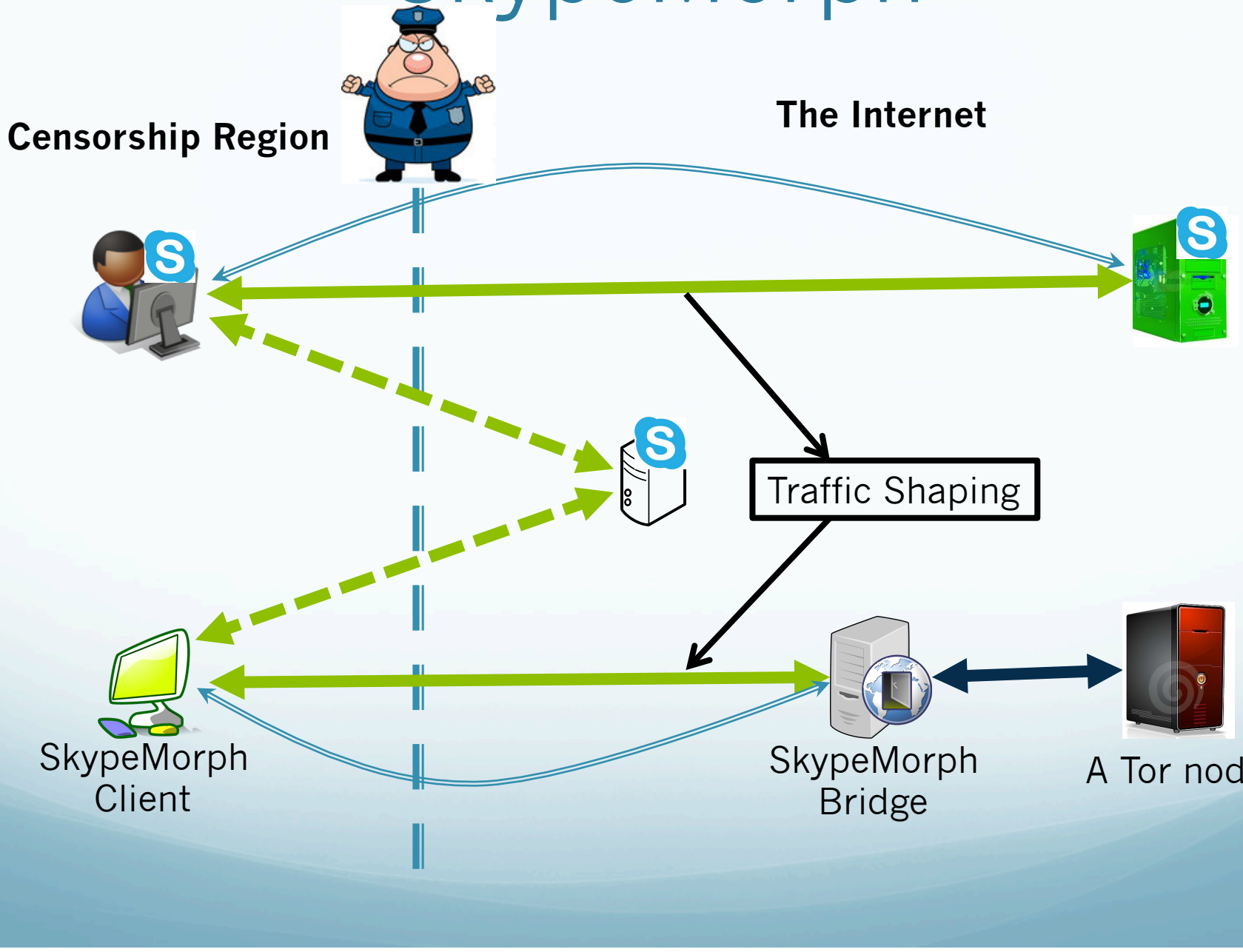


Parrot systems

- Imitate a popular protocol
  - SkypeMorph (CCS'12)
  - StegoTorus (CCS'12)
  - CensorSpoofer (CCS'12)


What's, uh...
What's wrong with it?
'E's dead, that's what's wrong with it!

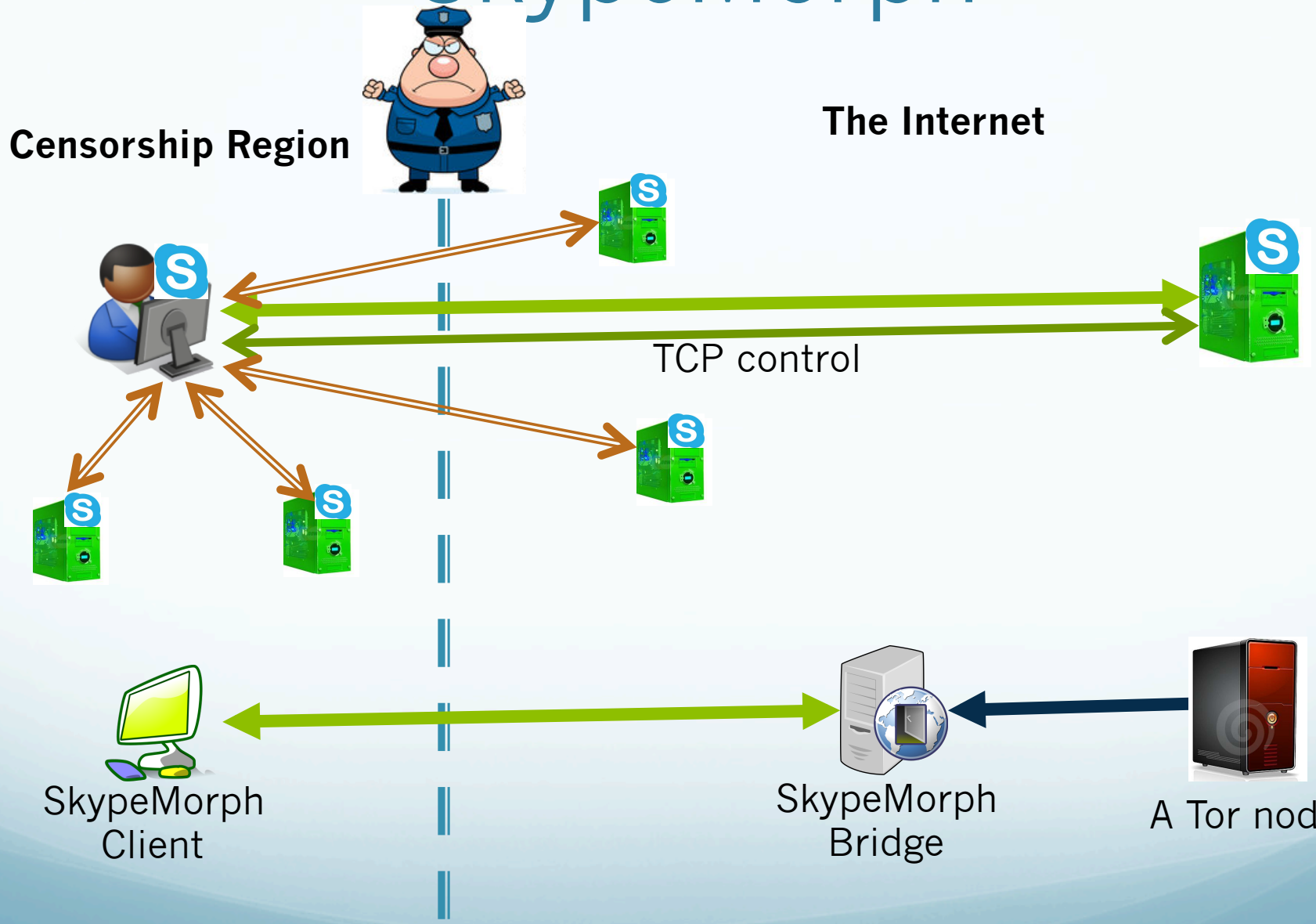
SkypeMorph


Censorship Region
The Internet
Traffic Shaping
SkypeMorph Client
SkypeMorph Bridge
A Tor node

SoM header

- The start of message (SoM) header field is MISSING!
- Single-packet identifier, instead of sophisticated statistical traffic analysis

SkypeMorph


Censorship Region
The Internet
TCP control
SkypeMorph Client
SkypeMorph Bridge
A Tor node

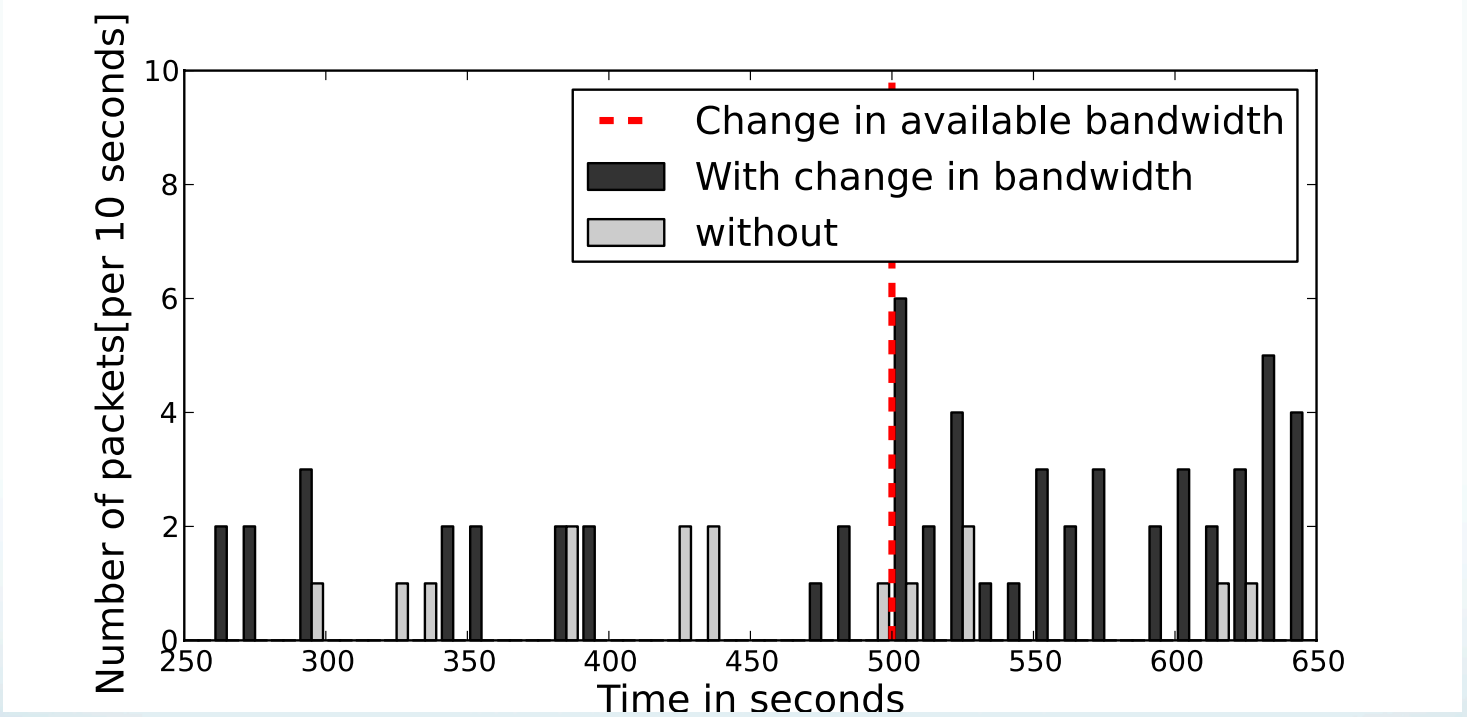

No, no.....No,
'e's stunned!

SkypeMorph+

Let's imitate the missing!

- Hard to mimic dynamic behavior
  - Active/proactive tests

Dropping UDP packets

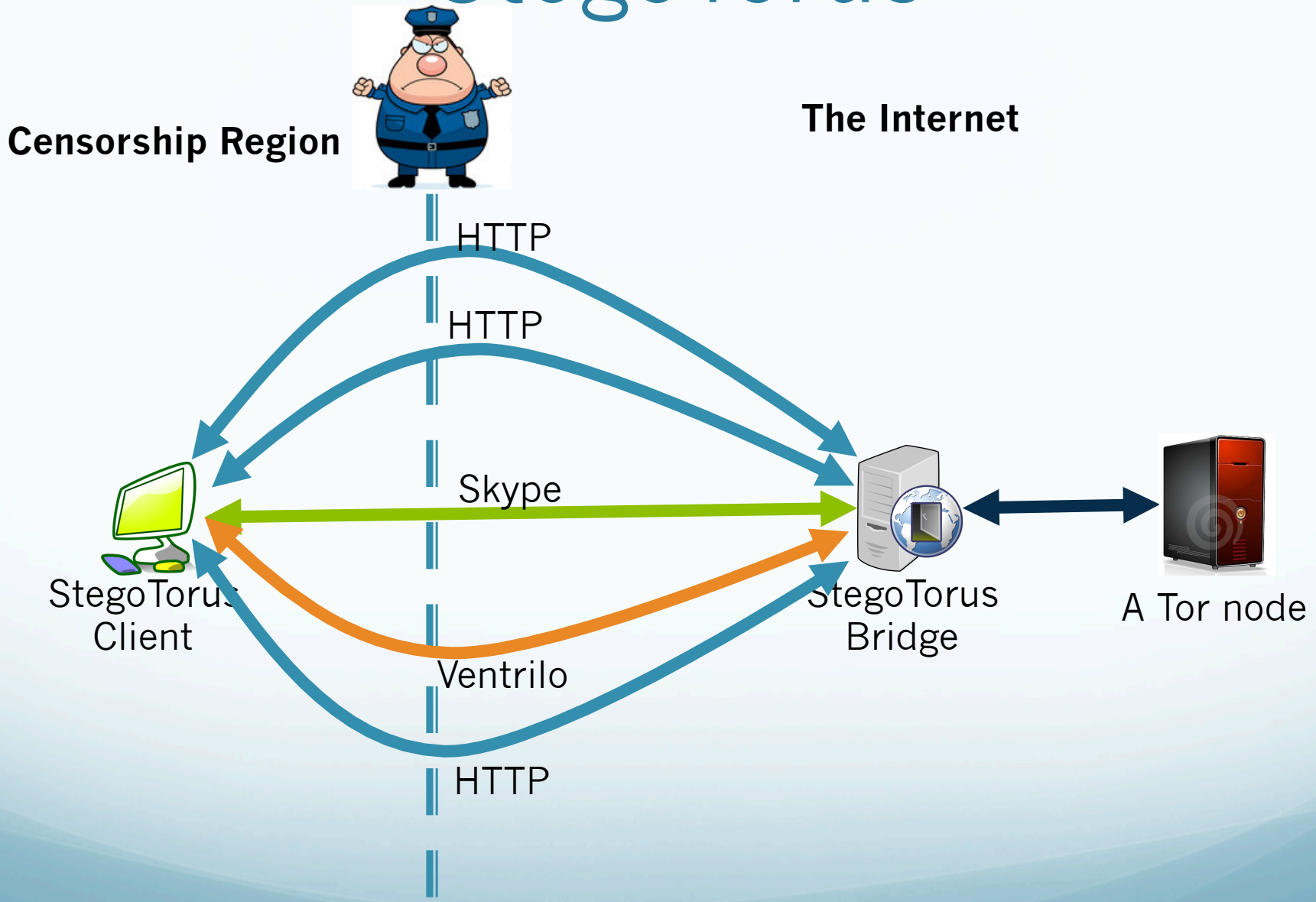


Other tests

Test	Skype	SkypeMorph+
Flush Supernode cache	Serves as a SN	Rejects all Skype messages
Drop UDP packets	Burst of packets in TCP control	No reaction
Close TCP channel	Ends the UDP stream	No reaction
Delay TCP packets	Reacts depending on the type of message	No reaction
Close TCP connection to a SN	Initiates UDP probes	No reaction
Block the default TCP port	Connects to TCP ports 80 and 443	No reaction

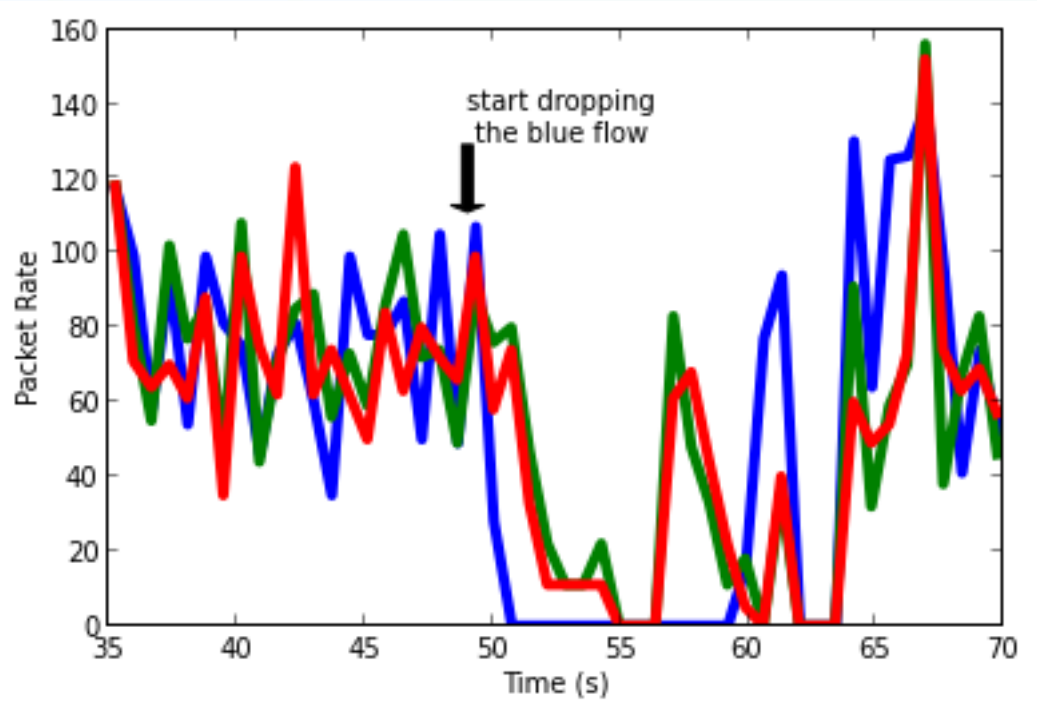

Now that's what
I call a dead parrot.

StegoTorus


Censorship Region
The Internet
HTTP
HTTP
Skype
Ventrilo
HTTP
StegoTorus Client
StegoTorus Bridge
A Tor node

StegoTorus chopper

- Dependencies between links



StegoTorus-Skype

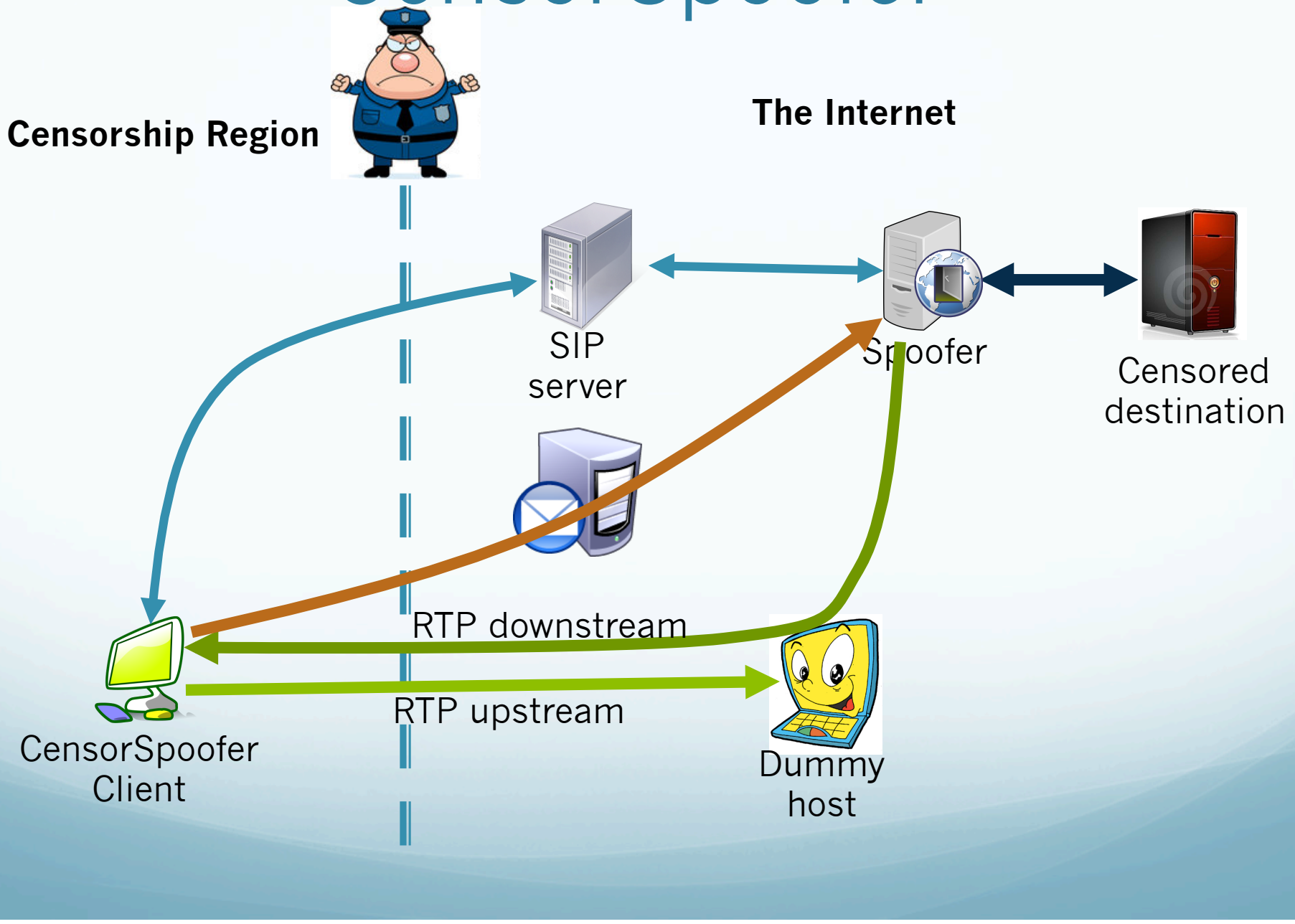
- The same attacks as SkypeMorph
  - Even more attacks!

StegoTorus-HTTP

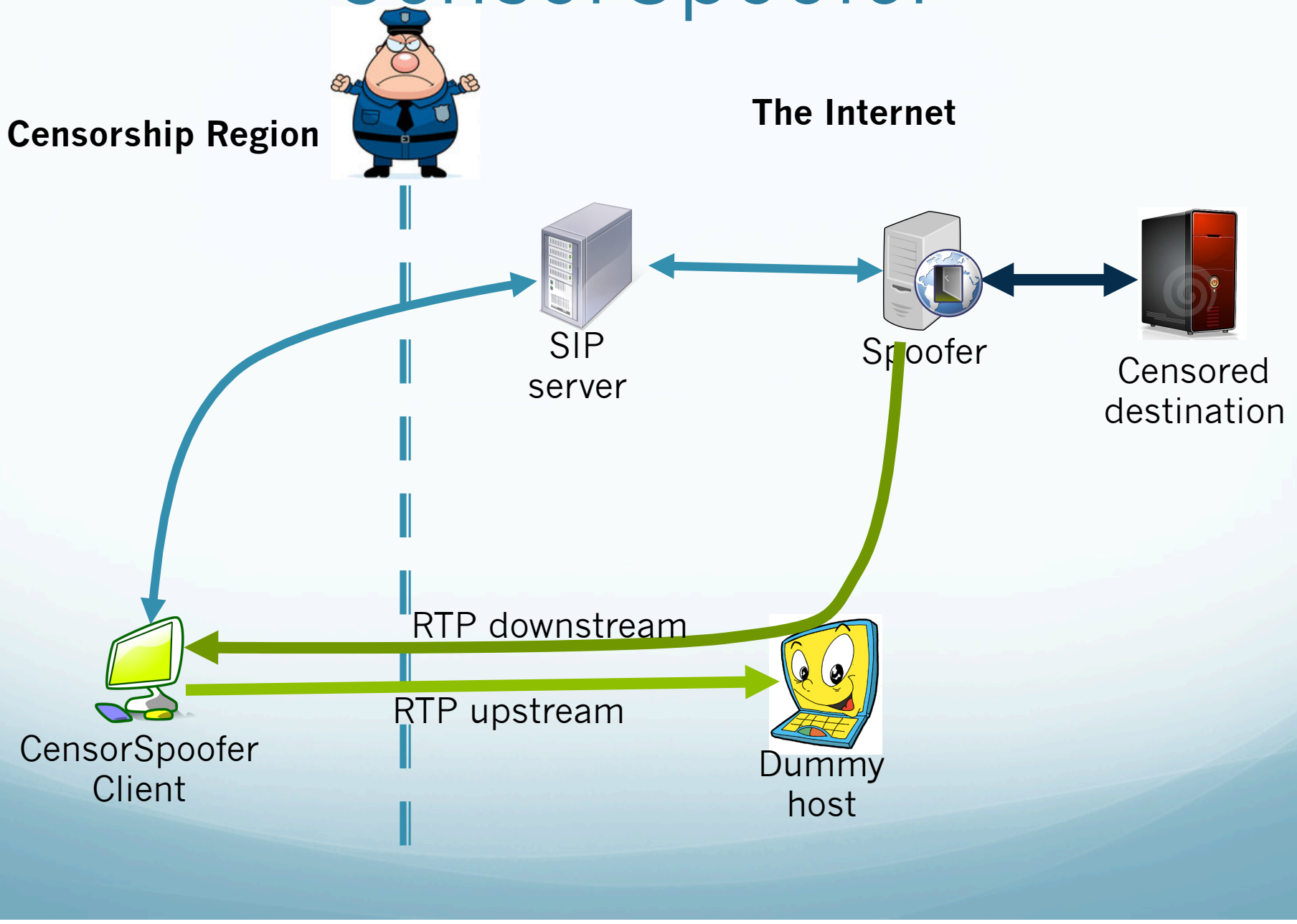
- Does not look like a typical HTTP server!
- Most HTTP methods not supported!

HTTP request	Real HTTP server	StegoTorus's HTTP module
GET existing	Returns "200 OK" and sets `Connection` to `keep-alive`	Arbitrarily sets `Connection` to either `keep-alive` or `Close`
GET long request	Returns "404 Not Found" since URI does not exist	No response
GET non-existing	Returns "404 Not Found"	Returns "200 OK"
GET wrong protocol	Most servers produce an error message, e.g., "400 Bad Request"	Returns "200 OK"
HEAD existing	Returns the common HTTP headers	No response
OPTIONS common	Returns the supported methods in the Allow line	No response
DELETE existing	Most servers have this method not activated and produce an error message	No response
TEST method	Returns an error message, e.g., "405 Method Not Allowed" and sets `Connection=Close`	No response
Attack request	Returns an error message, e.g., "404 Not Found"	No response

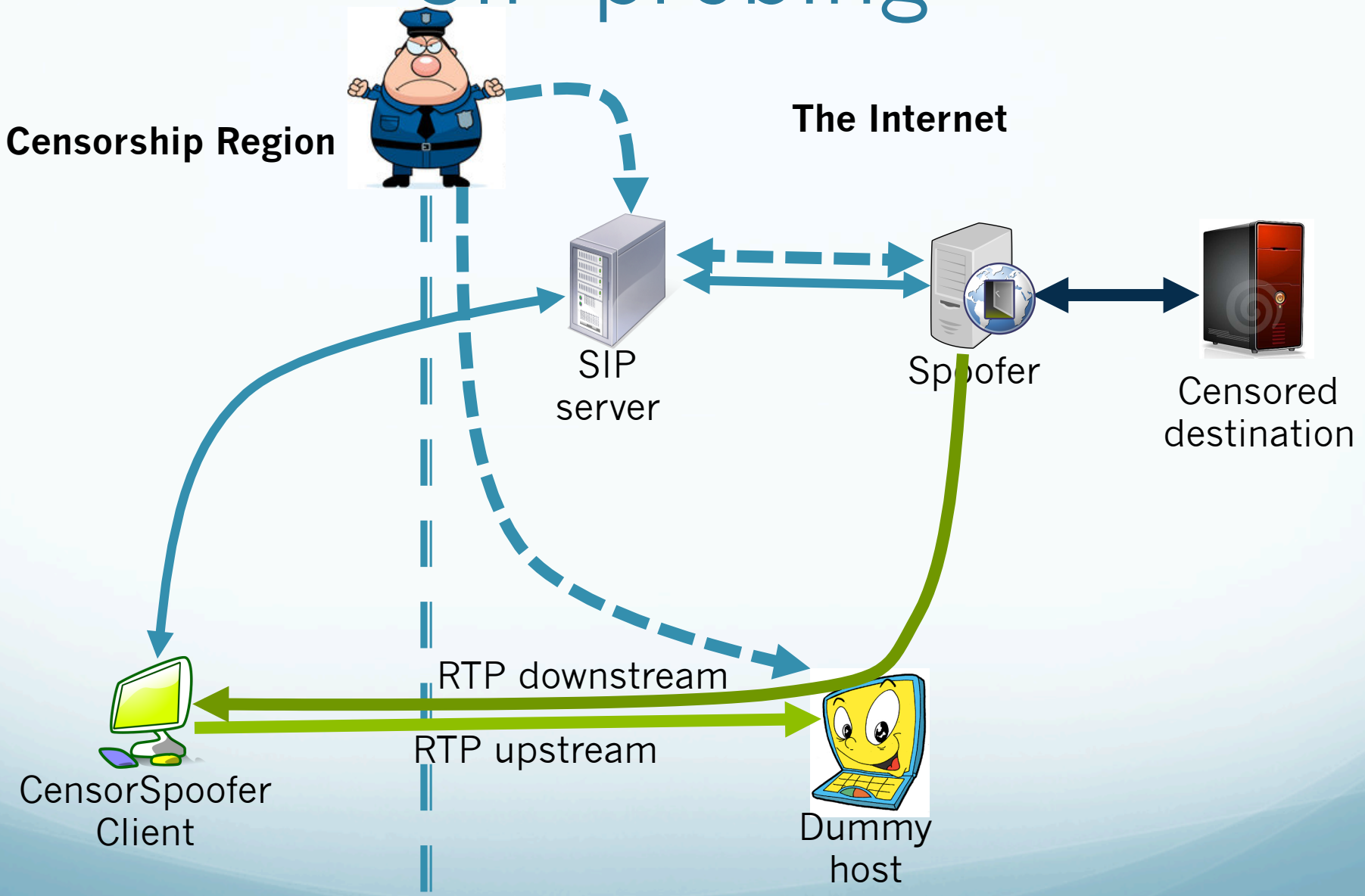
CensorSpoofer



CensorSpoofer



SIP probing


Censorship Region
The Internet
SIP
server
Spoofer
Censored
destination
RTP downstream
RTP upstream
CensorSpoofer
Client
Dummy
host


No no!
'E's pining!
'E's not pinin'!
'E's expired and gone to meet 'is maker!

Lesson 1

Unobservability by imitation is fundamentally flawed!

Imitation Requirements

Correct	**SideProtocols**
IntraDepend	**InterDepend**
Err	**Network**
Content	**Patterns**
Users	**Geo**
Soft	**OS**

Lesson 2

Partial imitation is worse than no imitation!

Alternative

- Do not imitate, but **Run** the target protocol
  - IP over Voice-over-IP [NDSS'13]
  - Challenge: efficiency

This is an ex-parrot!
This parrot is no more
This is a late parrot
It's stone dead