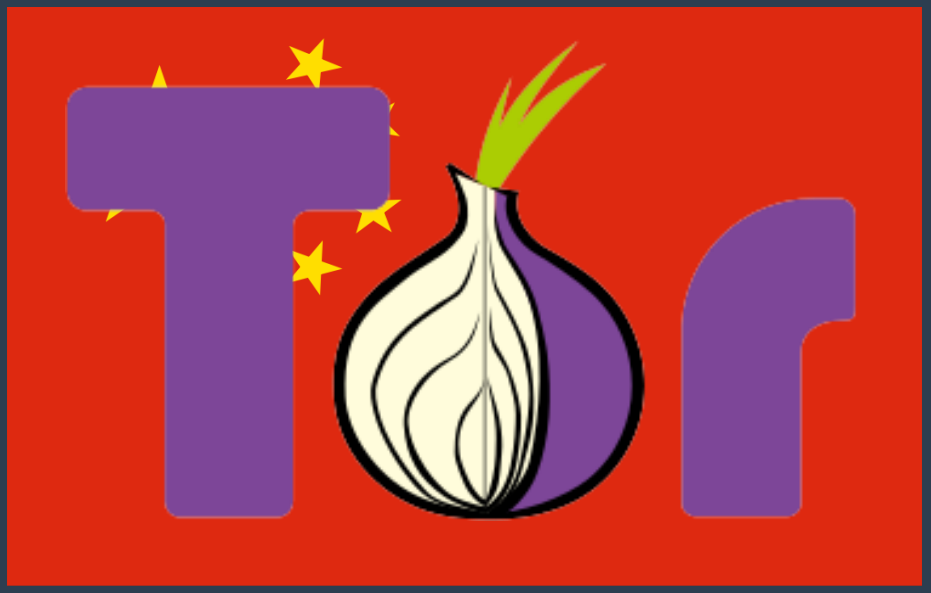
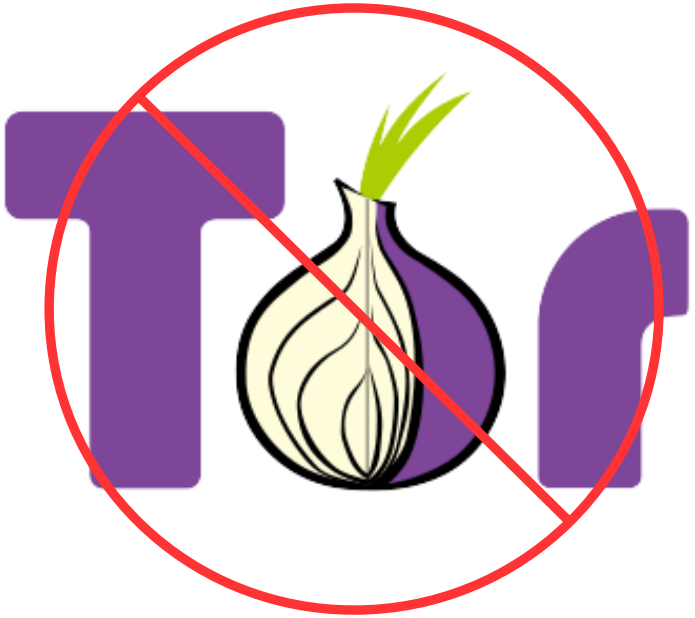
Analyzing China's Blocking of Unpublished Tor Bridges



Arun Dunna, Ciarán O'Brien, Phillipa Gill
University of Massachusetts Amherst

The Digital Arms Race



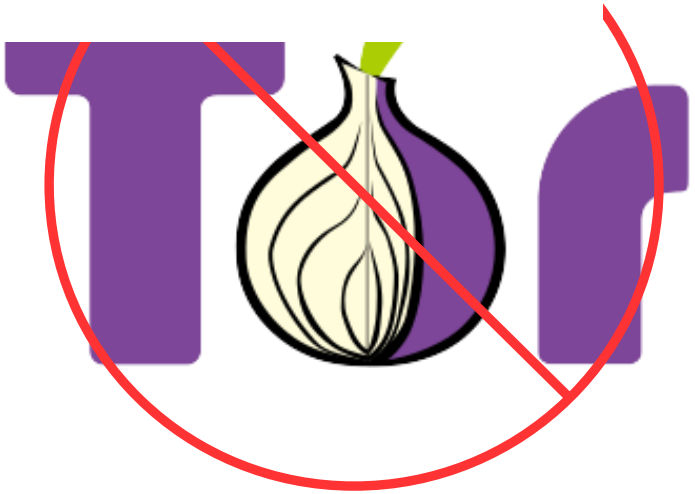


The Digital Arms Race

Berkeley SCHOOL OF INFORMATION

Tor and the Censorship Arms Race: Lessons Learned





The Digital Arms Race

Berkeley SCHOOL OF INFORMATION

The Register® Biting the hand that feeds IT

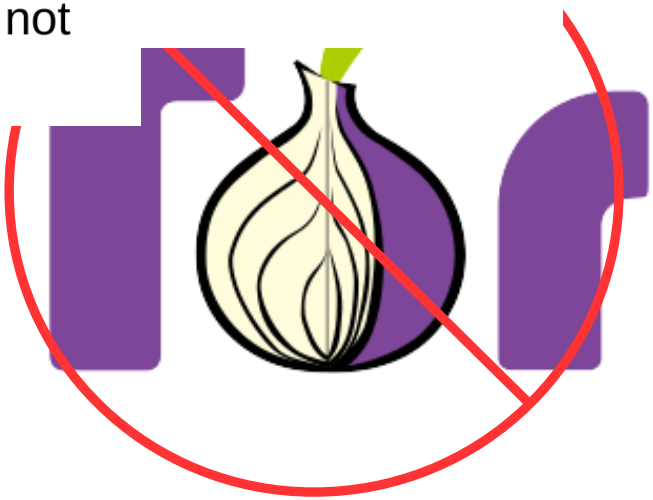
Security

Russia, China vow to kill off VPNs, Tor browser

New laws needed because today's censorship not good enough, apparently



ms Race:



The Digital Arms Race

Berkeley SCHOOL OF INFORMATION

Security

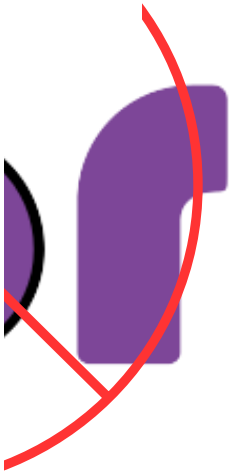
Russia, China

The Register®

Columbia Journalism Review.

The voice of journalism

In China, an entire generation is growing up with censored internet



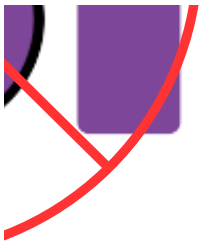
The Digital Arms Race

WIRED

LILY HAY NEWMAN SECURITY 08.04.17 10:00 AM

THE ATTACK ON GLOBAL PRIVACY LEAVES FEW PLACES TO TURN

up with censored internet



The Digital Arms Race



Prior Work

	2012	2015
Block Method	(IP, Port)	(IP, Port)
Block Duration	12 hours	12 hours
Scanning Queues	15 minutes	Instantly
Scanner Distribution	Non-Uniform	Uniform
Most Common Scanner	202.108.181.70	202.108.181.70
Common Scanner ASes	4134, 4837, 17622	4134, 4837, 7497

- 2012 FOCI – P. Winter and S. Lindskog
- 2015 IMC – Ensafi et al.
- Now 2018 – what's changed?

Setup



Setup



Tor Bridge



Setup



Tor Bridge



Tor Relay



Setup



Tor Bridge



Tor Relay



Tor Client



Public Network Reachability



Tor Client



Consensus

Public Network Reachability

- Connect to consensus relays

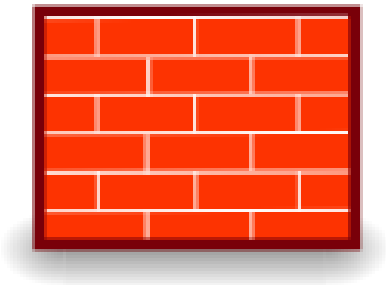


Public Network Reachability

- Connect to consensus relays **Blocked**



Tor Client





Consensus

Public Network Reachability

- Connect to consensus relays **Blocked**
- Ping public relays from client

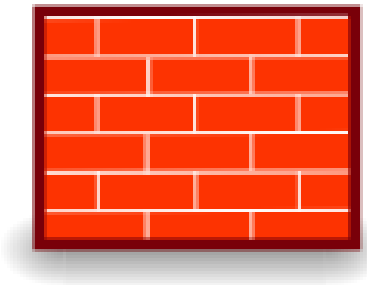


Public Network Reachability

- Connect to consensus relays **Blocked**
- Ping public relays from client **Blocked**



Tor Client





Consensus

Public Network Reachability

- Connect to consensus relays **Blocked**
- Ping public relays from client **Blocked**



Tor Client



Public Relay

Public Network Reachability

- Connect to consensus relays **Blocked**
- Ping public relays from client **Blocked**
- Published relays blocked after 10 minutes



Tor Client

Public Relay

Public Network Reachability

- Connect to consensus relays **Blocked**
- Ping public relays from client **Blocked**
- Published relays blocked after 10 minutes
- Blacklist purged after 12 hrs if Tor is stopped



Relay (Bridge) Blocking

Relay (Bridge) Blocking



Relay (Bridge) Blocking





Relay (Bridge) Blocking

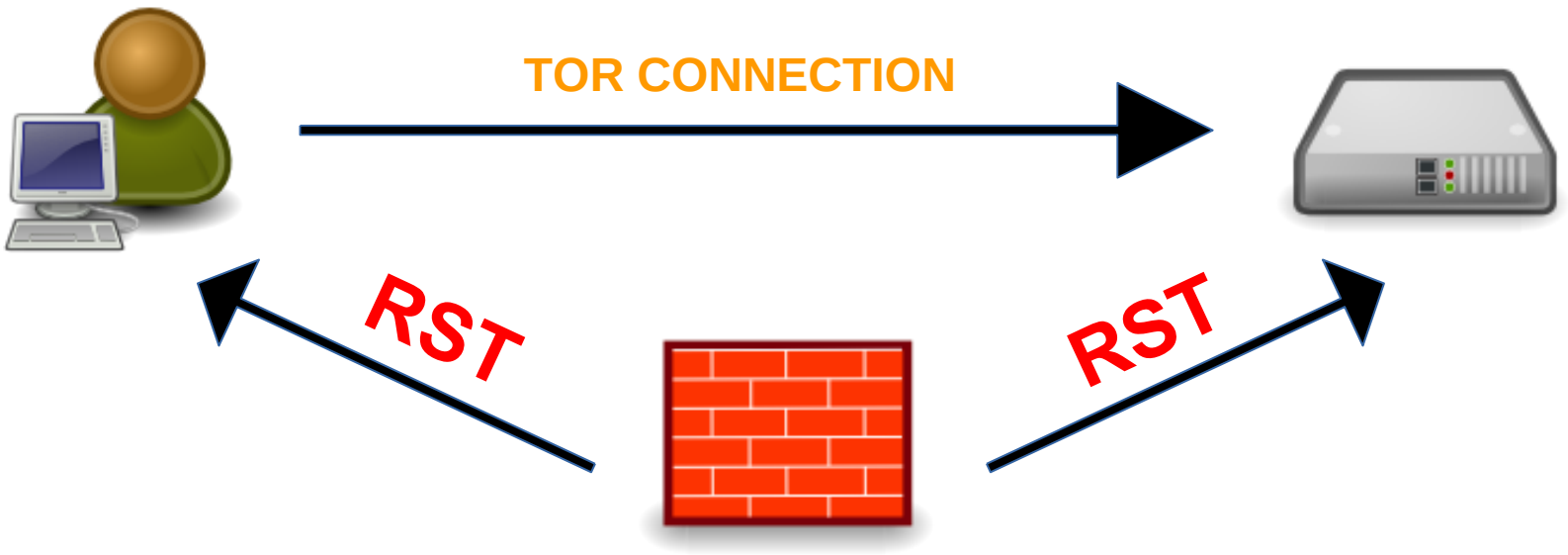


Relay (Bridge) Blocking



Relay (Bridge) Blocking

- Initial connection attempt blocked – RST



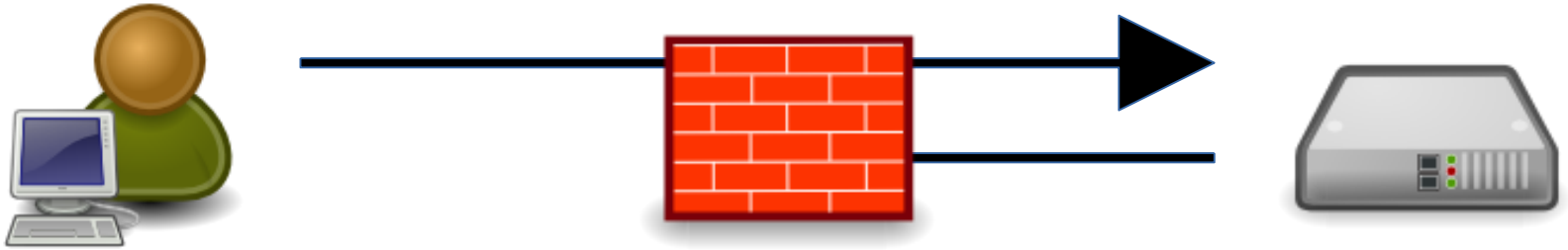
Relay (Bridge) Blocking

- Initial connection attempt blocked – RST



Relay (Bridge) Blocking

- Initial connection attempt blocked – RST
- Blocks relays at IP level (not port like 2012, 2015) – unidirectional (bridge to client blocked)

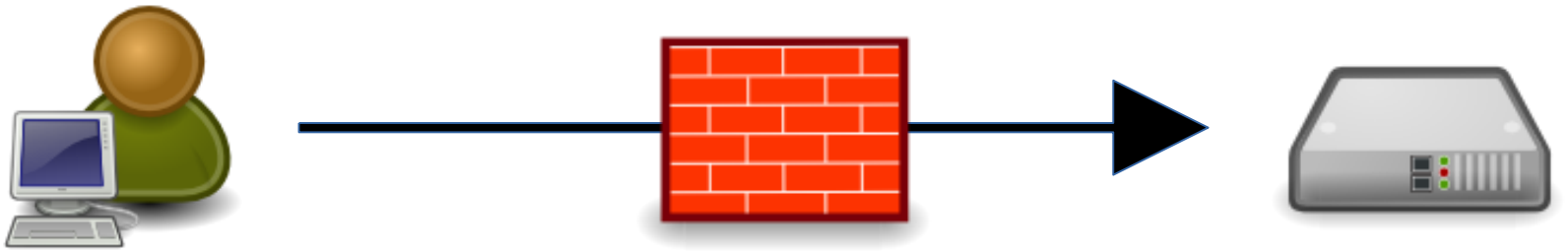


Blocking Duration



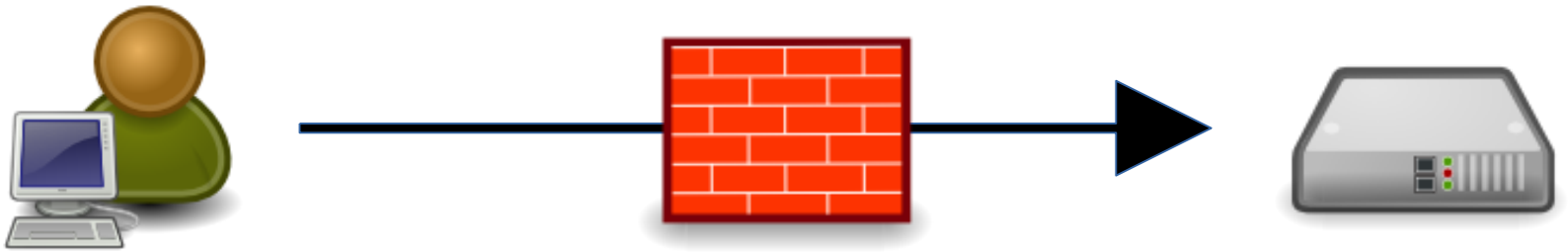
RUNNING
TOR

Blocking Duration



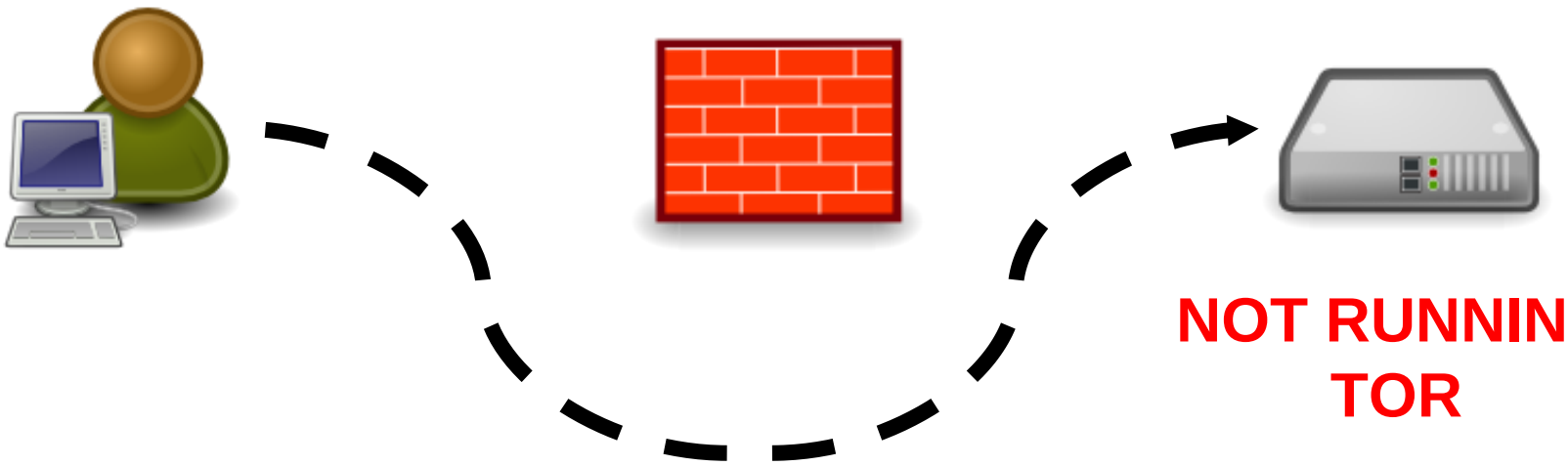
RUNNING
TOR

Blocking Duration

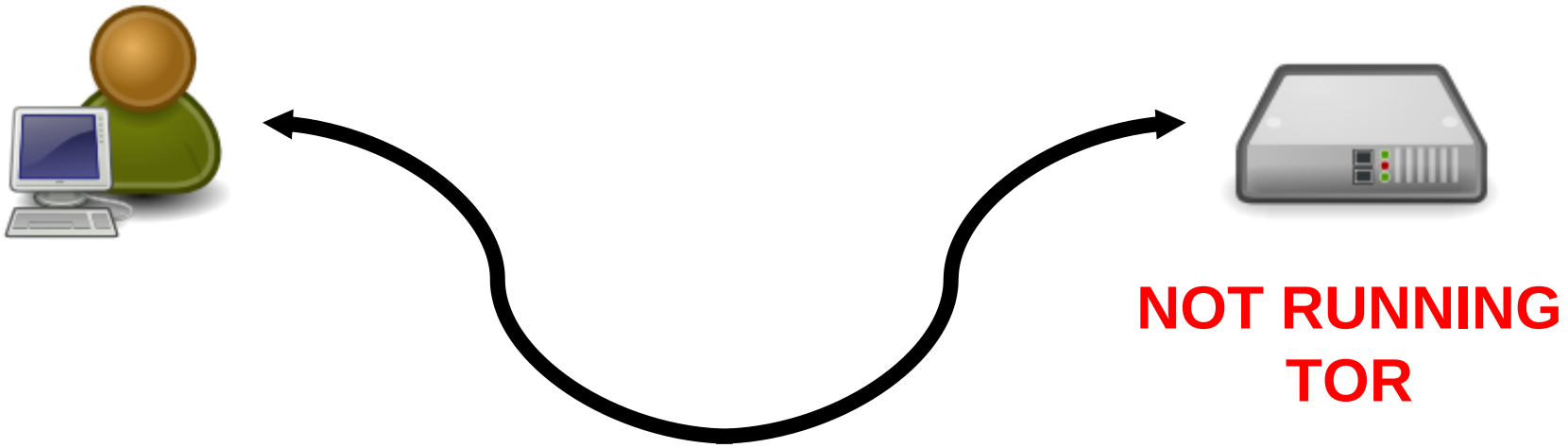


NOT RUNNING
TOR

Blocking Duration

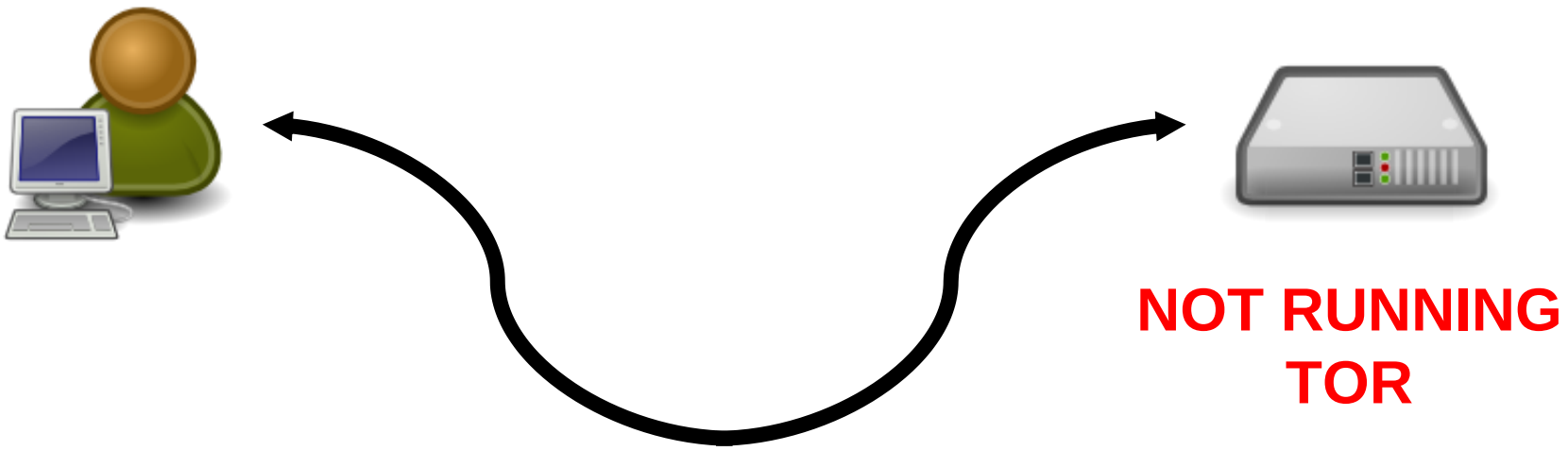


Blocking Duration



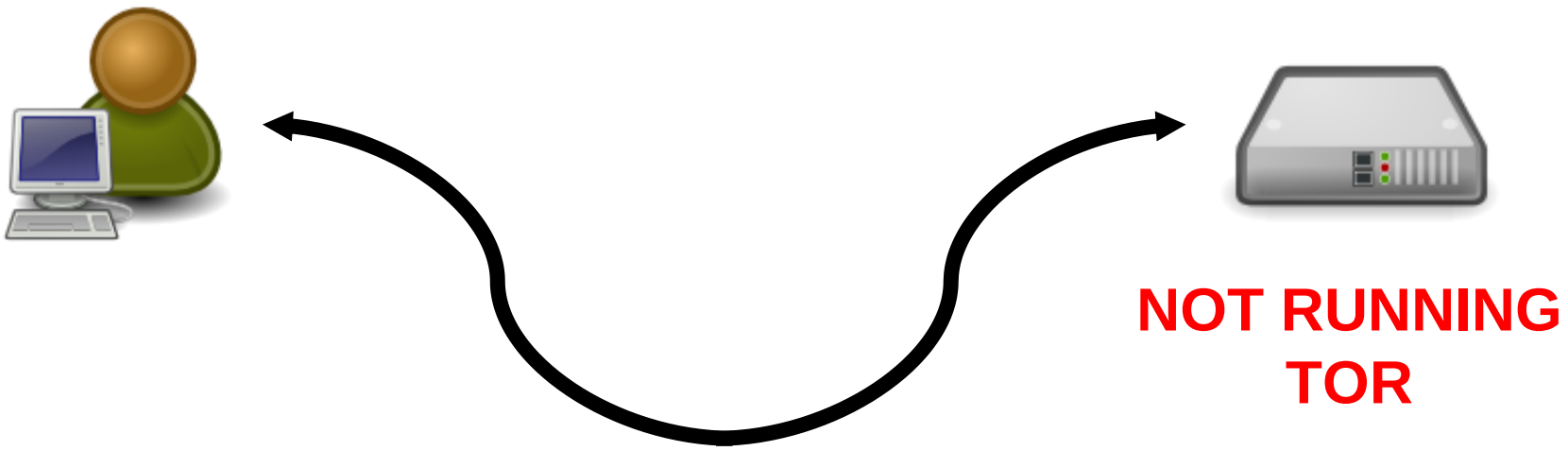
Blocking Duration

- Blocked for 12 hours, scanned in 12 hour intervals



Blocking Duration

- Blocked for 12 hours, scanned in 12 hour intervals
- GFW scans every 12 hours and IP blacklists – resource conservation?



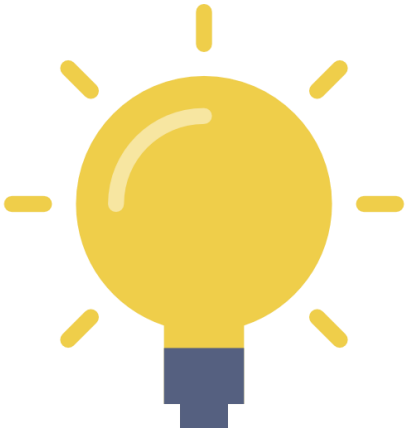
Fingerprinting - Setup

Fingerprinting - Setup

- Blocks IP, not ports, so cannot use one IP with multiple Tor services across multiple ports
- A method to attract scanners without getting blocked?

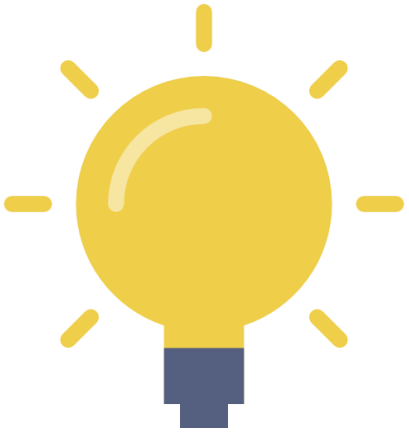
Fingerprinting - Setup

- Blocks IP, not ports, so cannot use one IP with multiple Tor services across multiple ports
- A method to attract scanners without getting blocked?



Fingerprinting - Setup

- Blocks IP, not ports, so cannot use one IP with multiple Tor services across multiple ports
- A method to attract scanners without getting blocked?



- Drop scanner packets – “we’re not a relay!”
- Over 44 hours… collected 934 unique IPs

Fingerprinting - Comparison

- Comparison of captured TCP SYN packets

	2015	2018
TTL Range	46 - 51	48 - 50
MSS Values	1400, 1460	1368, 1400
Window Scaling	7	7
Permit Selective ACKs	Yes	Yes
TCP Timestamp	Yes	Yes
No Operation Flag	Yes	Yes

Fingerprinting - Comparison

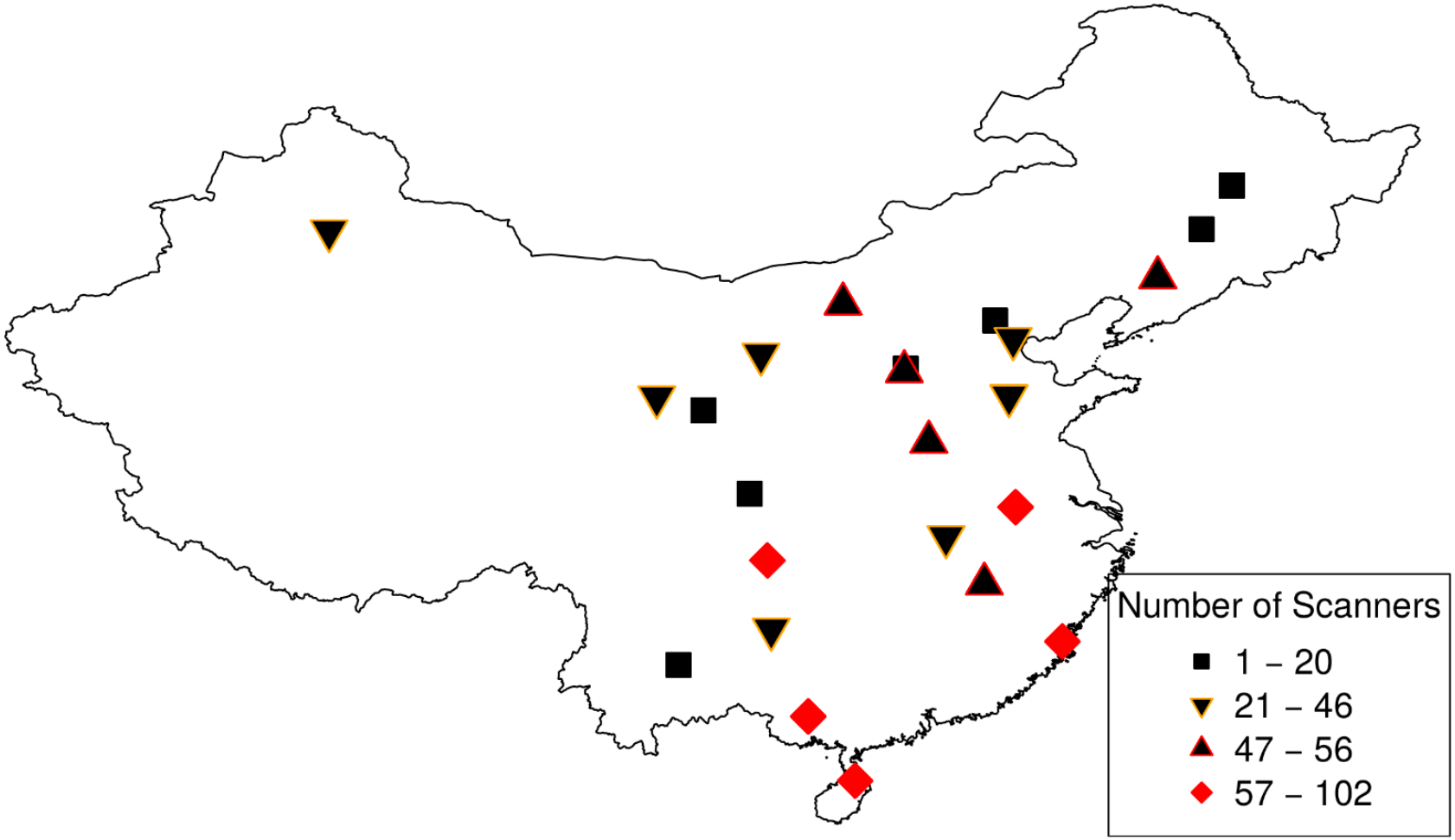
- Comparison of captured TCP SYN packets

	2015	2018
TTL Range	46 - 51	48 - 50
MSS Values	1400, 1460	1368, 1400
Window Scaling	7	7
Permit Selective ACKs	Yes	Yes
TCP Timestamp	Yes	Yes
No Operation Flag	Yes	Yes

- 111.202.242.93 is origin of 5% of SYN packets
- All of them have MSS of 1368, and we respond to them normally, but we're not blocked - different scanner?

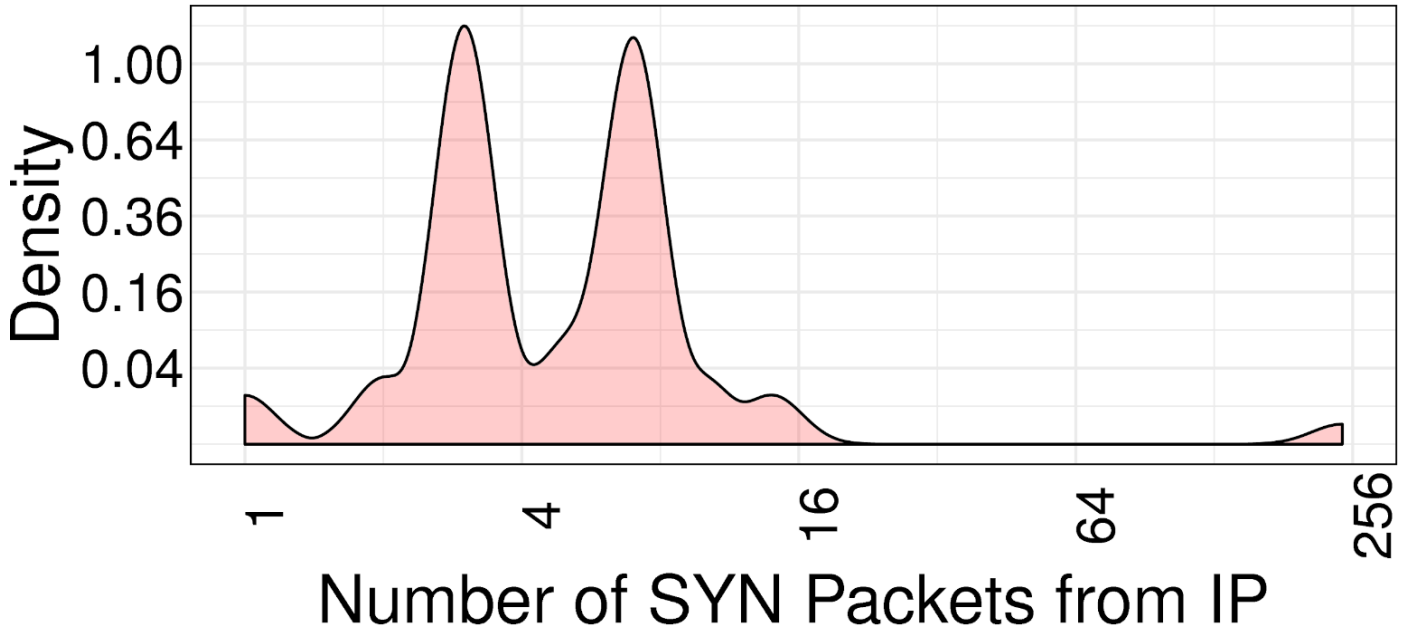
Fingerprinting - Infrastructure

- All scanners in China, geolocation using GeoLite2



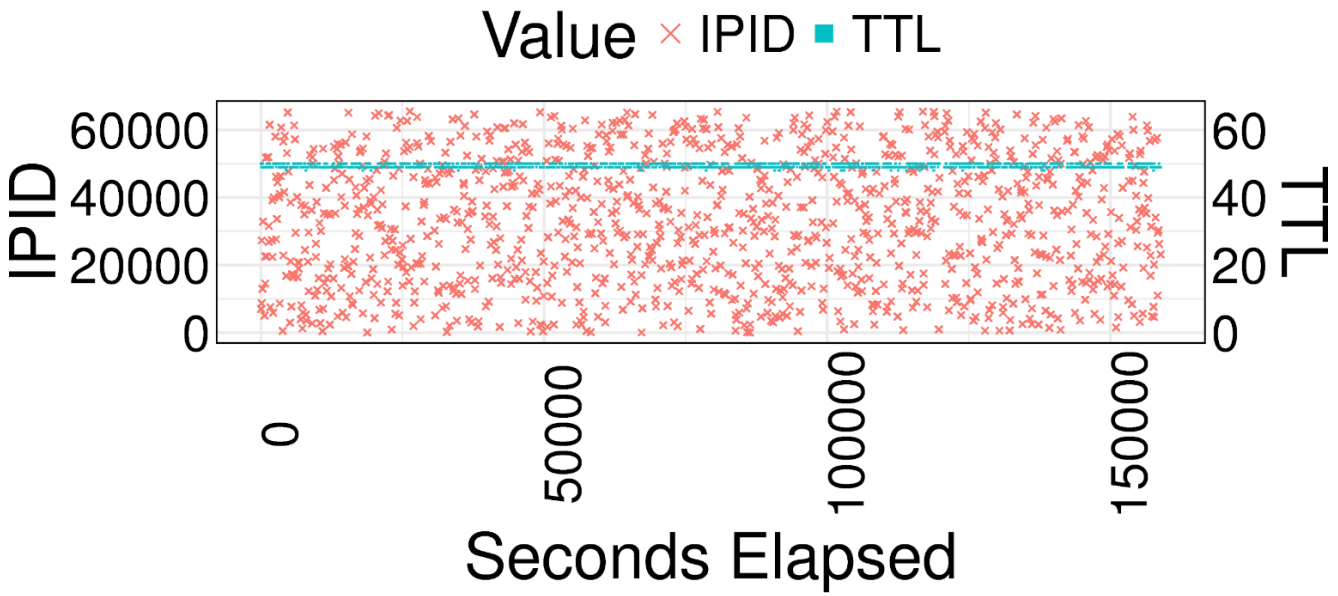
Fingerprinting - IPs

- Out of 934 IPs seen, 908 IPs conducted one scan, and 26 conducted two scans
- Each IP does one/two scans – avoiding detection?



Fingerprinting – IPID & TTL

- No trend in IPIDs observed… but similarity in TTL indicate colocation
- Cannot determine whether RST injectors are colocated with scanners (RSTs TTL 44, vs. 48-50)



Circumvention

Circumvention

- Pluggable Transports!

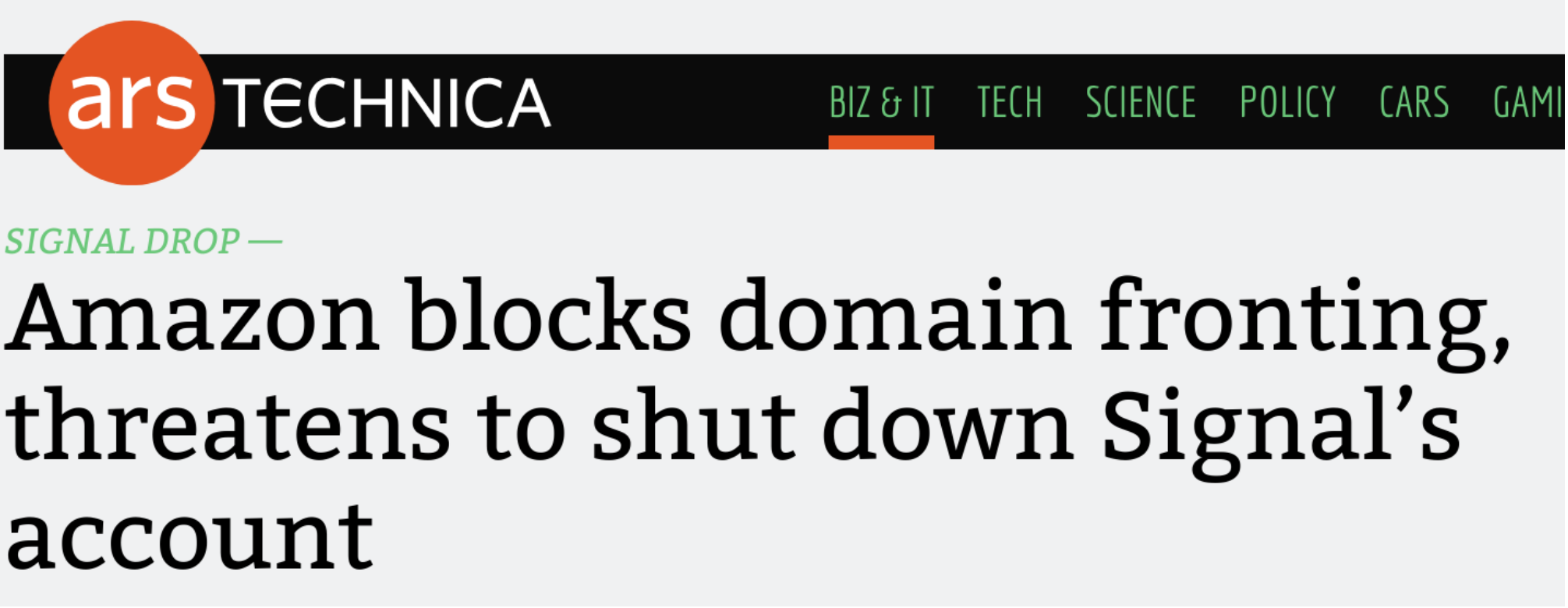
Circumvention

- **Pluggable Transports!**
  - Obfs4: obfuscation, not recommended due to bridge distribution

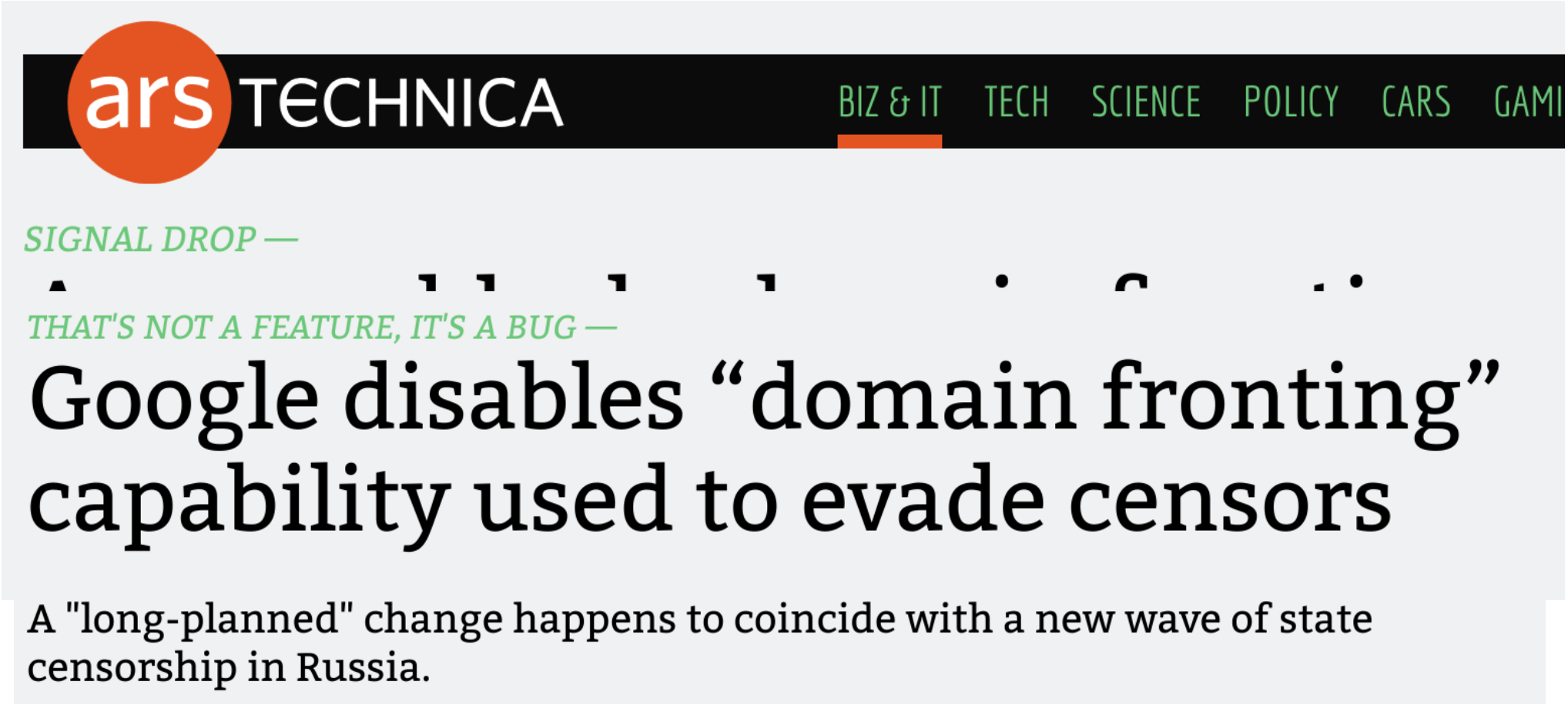
Circumvention

- **Pluggable Transports!**
  - Obfs4: obfuscation, not recommended due to bridge distribution
  - Meek: uses domain fronting, recommended for Chinese users… but how long?

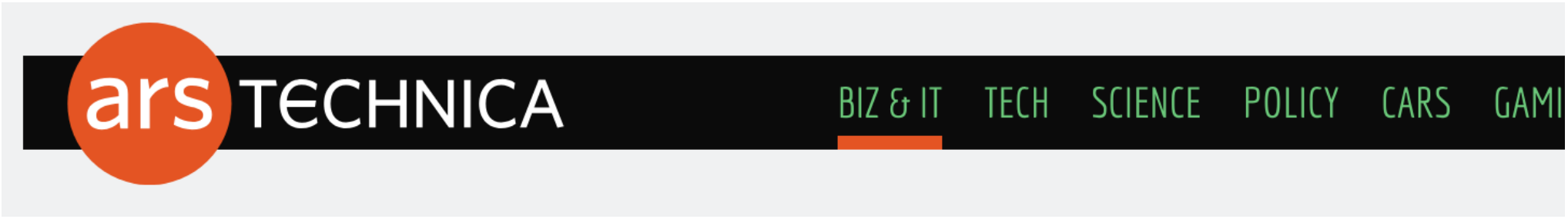
Circumvention



Circumvention



Circumvention



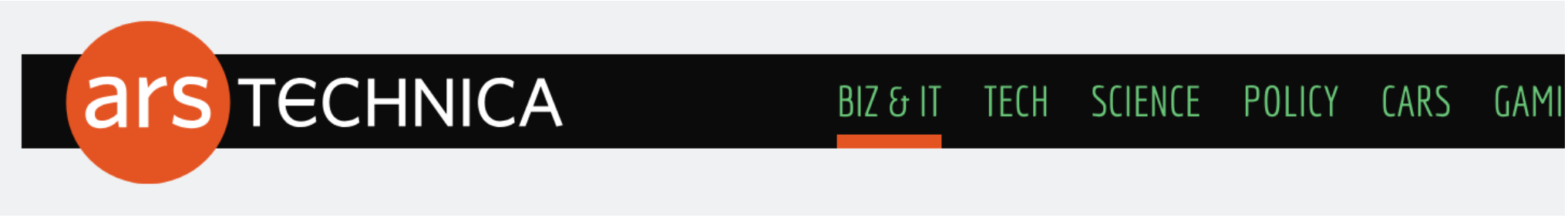
TECH INDUSTRY

Signal says Amazon, Google will no longer help it evade censorship

Hot on the heels of Google's move last week, Amazon Web Services said it will also switch off functionality for domain fronting.

A "long-planned" change happens to coincide with a new wave of state censorship in Russia.

Circumvention



TECH INDUSTRY

Signal says Amazon, Google will no longer help it evade censorship

Amazon Web Services starts blocking domain-fronting, following Google's lead

censorship in Russia.

Is there a better way?

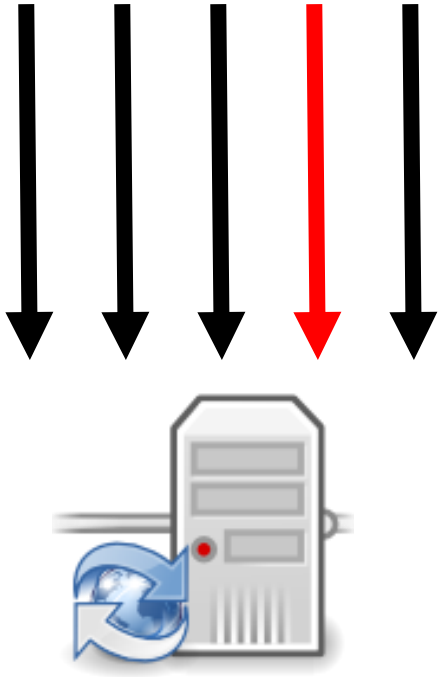
Rejecting Scanners

Rejecting Scanners

- Bridge relays drop packets from GFW scanners – “I’m not running Tor!”

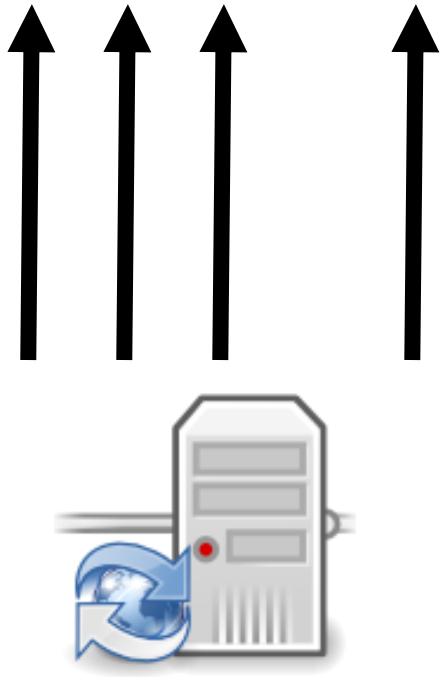
Rejecting Scanners

- Bridge relays drop packets from GFW scanners – "I'm not running Tor!"



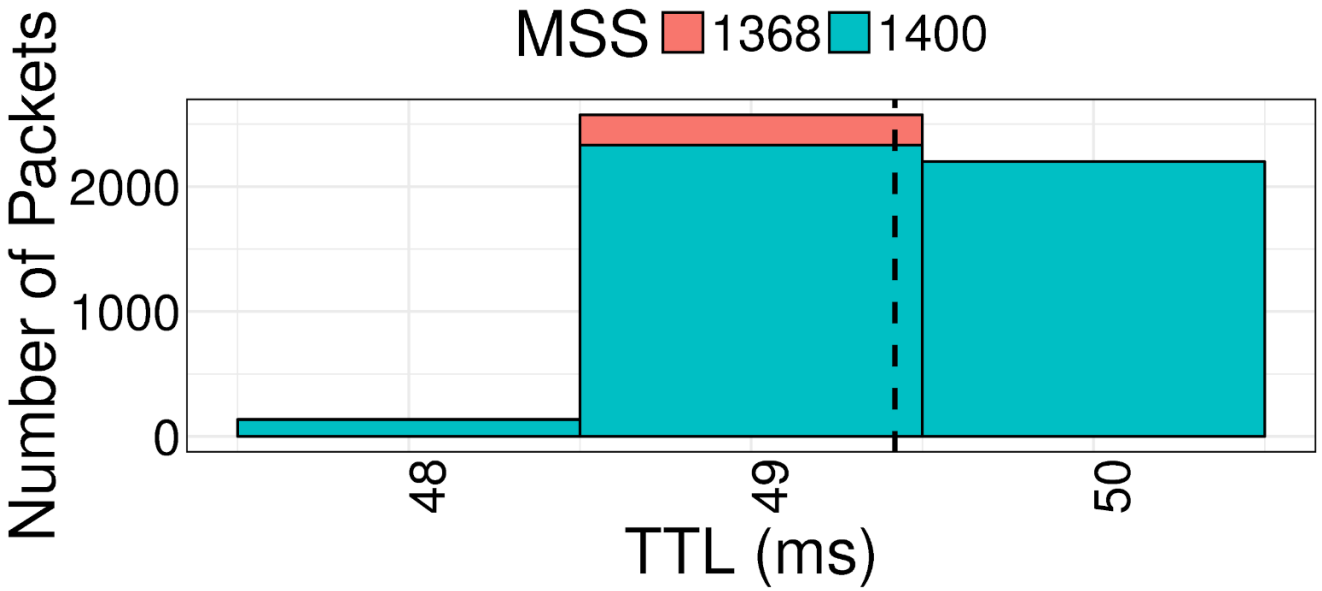
Rejecting Scanners

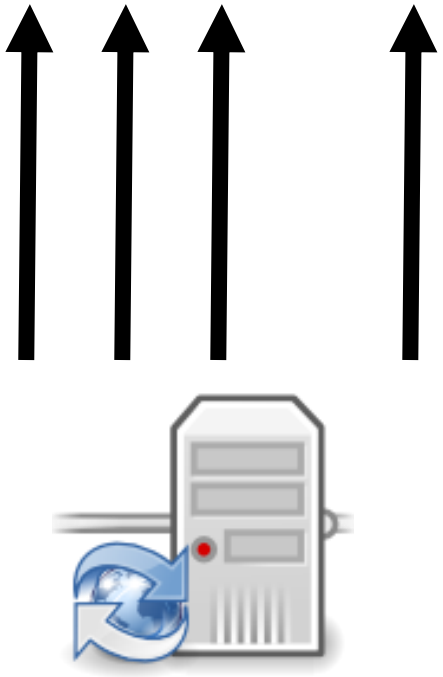
- Bridge relays drop packets from GFW scanners – "I'm not running Tor!"



Rejecting Scanners

- Bridge relays drop packets from GFW scanners – "I'm not running Tor!"
- EX: iptables -A INPUT -p tcp --destination-port 7412 -m tcpmss --mss 1400 -j DROP





Conclusion

- GFW now blocks by IP instead of (IP, Port), which makes measuring more challenging

Conclusion

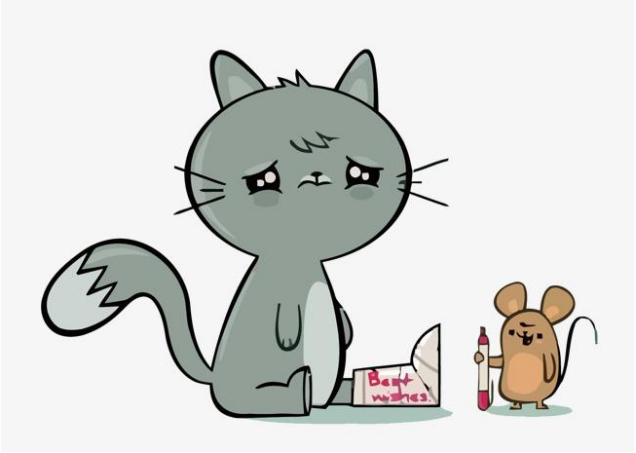
- GFW now blocks by IP instead of (IP, Port), which makes measuring more challenging
- Dropping scanner traffic results in bridge not getting blocked - how long until GFW responds?

Conclusion

- GFW now blocks by IP instead of (IP, Port), which makes measuring more challenging
- Dropping scanner traffic results in bridge not getting blocked - how long until GFW responds?
- Censor behavior changes over time, so it’s important to continue revisiting results

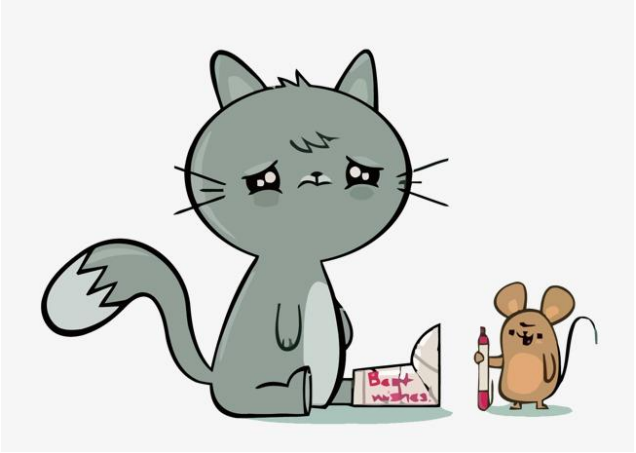
Conclusion

- GFW now blocks by IP instead of (IP, Port), which makes measuring more challenging
- Dropping scanner traffic results in bridge not getting blocked - how long until GFW responds?
- Censor behavior changes over time, so it’s important to continue revisiting results



Conclusion

- GFW now blocks by IP instead of (IP, Port), which makes measuring more challenging
- Dropping scanner traffic results in bridge not getting blocked - how long until GFW responds?
- Censor behavior changes over time, so it’s important to continue revisiting results





Thanks!

Arun Dunna – CS MS Student
adunna@cs.umass.edu

Calipr Lab, with Prof. Phillipa Gill
https://calipr.cs.umass.edu

We open source all of our datasets and code, available at https://calipr.cs.umass.edu, to maintain reproducibility.

Q/A

References

- Images
  - https://github.com/hjnilsson/country-flags
  - http://www.opensecurityarchitecture.org/cms/library/icon-library
  - https://www.flaticon.com/authors/smashicons
  - https://trac.torproject.org/projects/tor/attachment/wiki/doc/meek/meek-diagram.svg