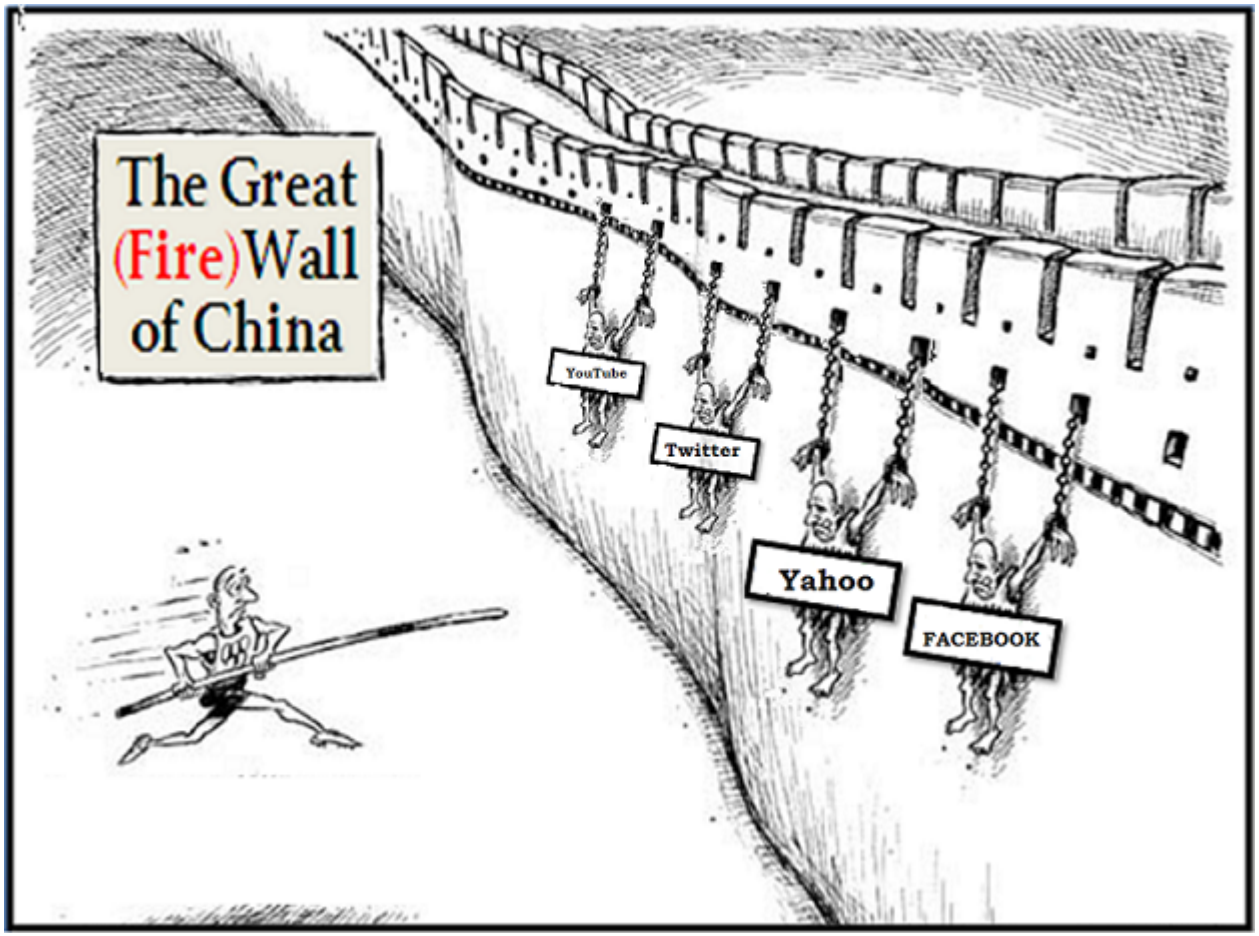
institute imdea software

www.software.imdea.org

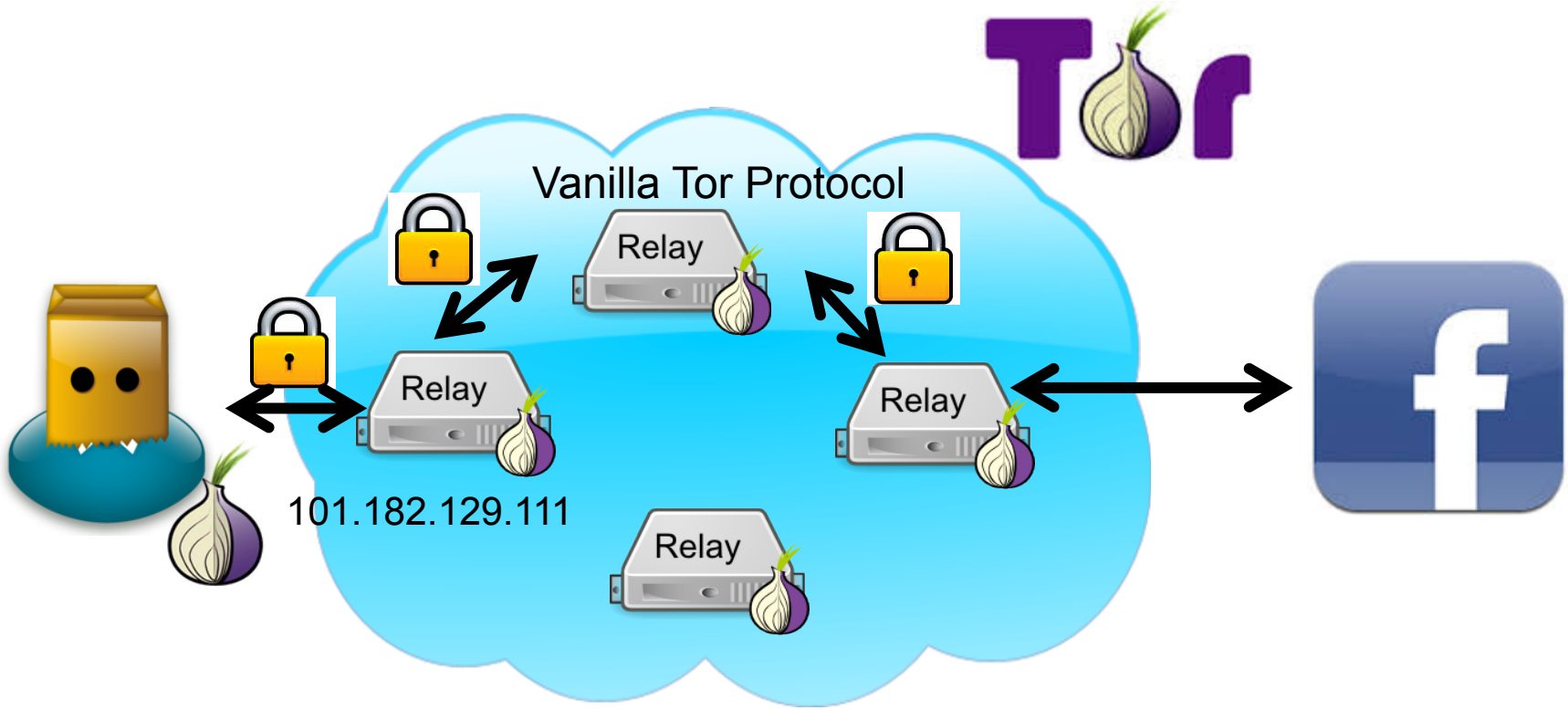
Dissecting Tor Bridges: a Security Evaluation of Their Private and Public Infrastructures

Srdjan Matic, Carmela Troncoso, Juan Caballero

Internet Censorship

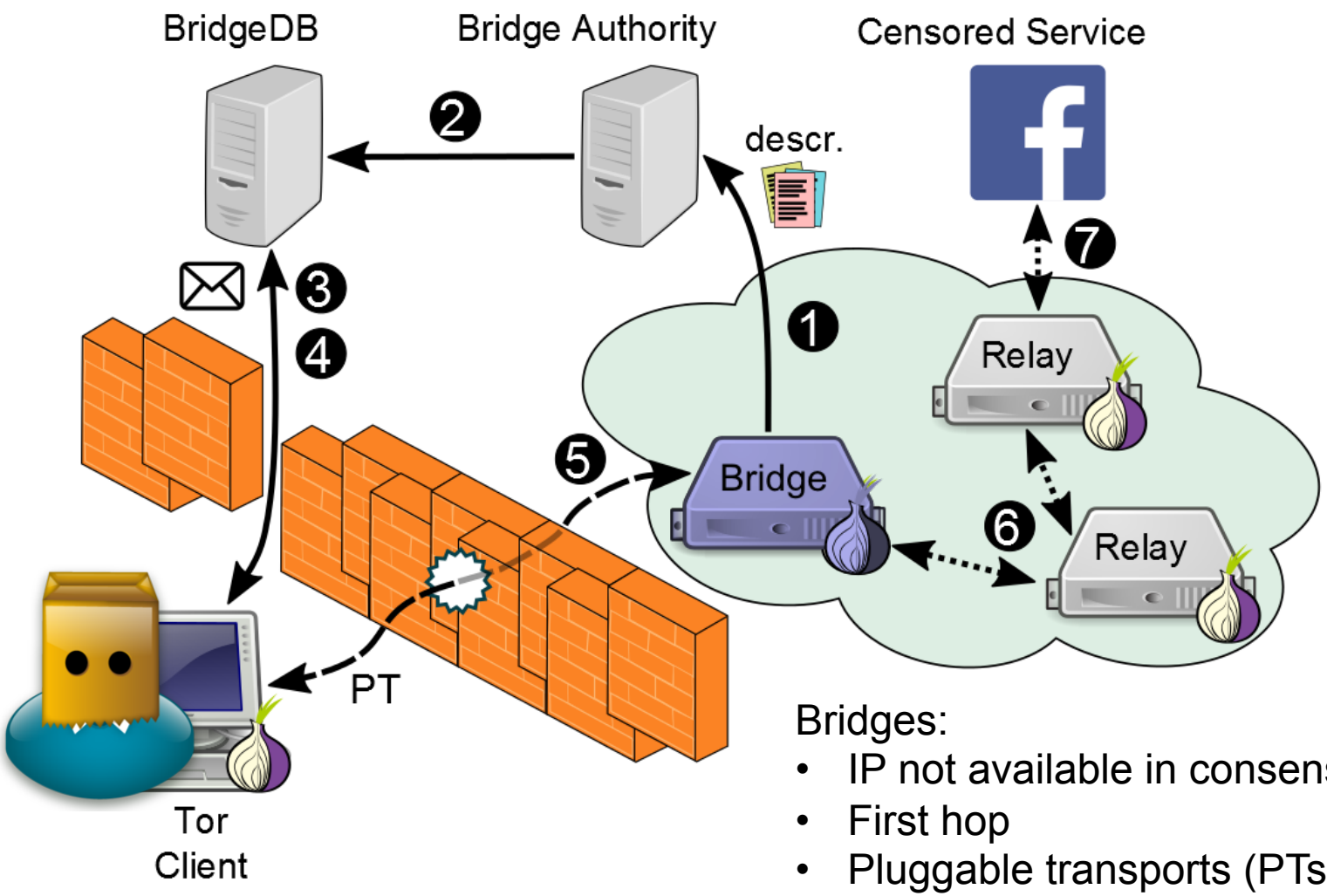


Onion Routing



http://facebook.com

Tor Bridges

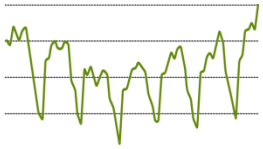


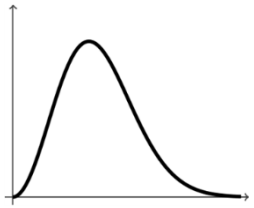
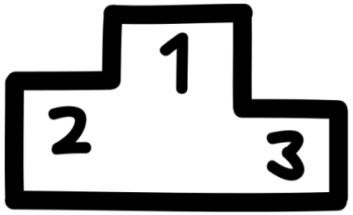
Bridges:

- IP not available in consensus
- First hop
- Pluggable transports (PTs)
- Public or private
- Default bridges

Our Goals

- Perform first systematic study of the security of the Tor bridge infrastructure
  - Public bridges

  - Private bridges
  - Private proxies



Known Tor Issues

Two issues known to Tor project since October 2010

1. Vanilla Tor Certificates
   - Vanilla Tor uses TLS handshake
   - Easy to spot certificates
   - It won't be fixed

2. Open OR Port
   - Bridges have open OR Port with Vanilla Tor
   - Even if they do not offer Vanilla Tor
   - Difficult to fix

Outline

Intro

Approach

Public Bridge Analysis

Private Bridge Analysis

Datasets

SHODAN

Scan 200+ ports with multiple protocols
19 ports scanned with TLS
Indexed data available

censys

Scan 6 ports with TLS
Raw + indexed data available

Identify candidate bridge IP addresses (without scanning ourselves)

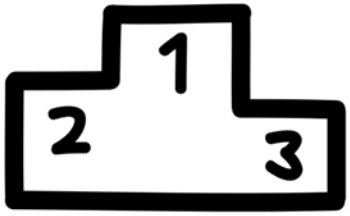
COLLECTor

Node-level data on public bridges + relays
Some bridge data sanitized

Is there sensitive data not anonymized?

Discovering Bridges

1. Finding candidate IP addresses
2. Filtering relays
3. Verifying IP addresses
4. Identifying private proxies
5. Classifying as public or private bridge



Outline

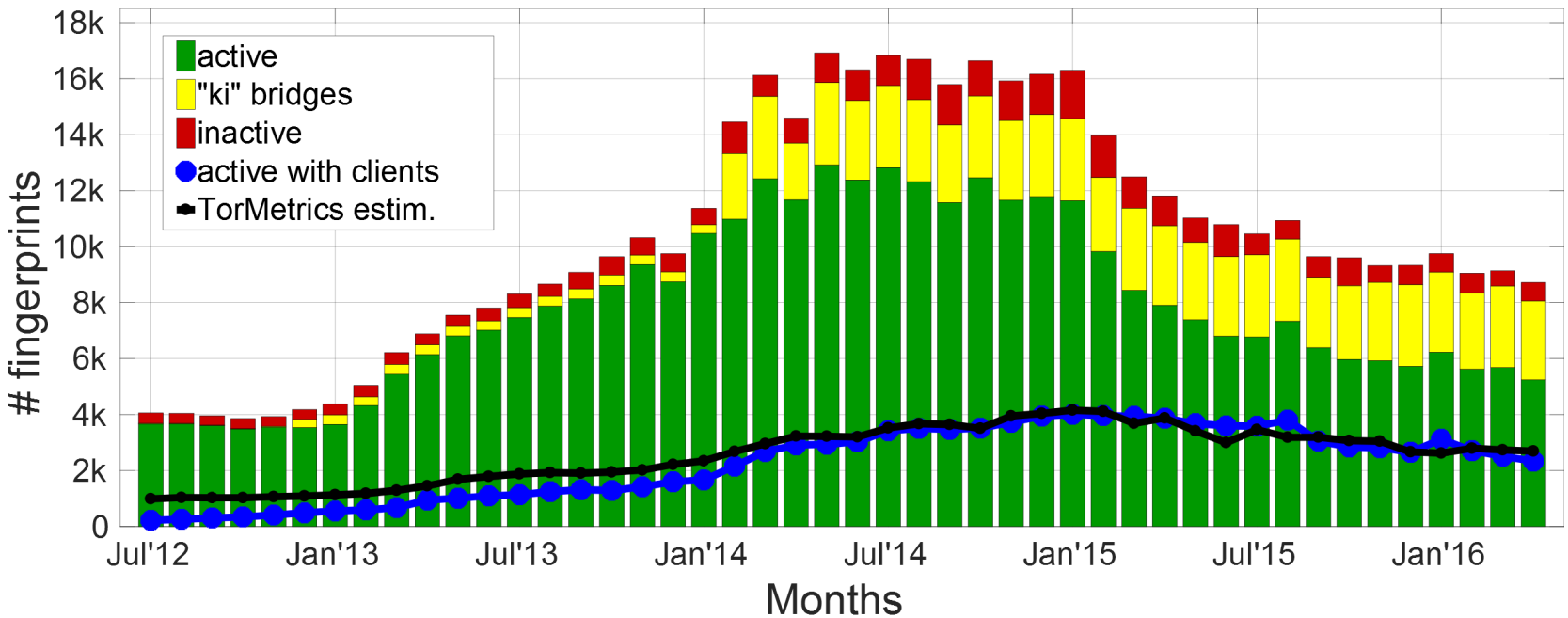
Intro

Approach

Public Bridge Analysis

Private Bridge Analysis

Bridge Population



April 2016:

- 5.3K active public bridges
- 2.3K bridges with clients

Different population metrics!

Bridge Stability

Current censor block policies that remove blocks every 25 hours are **very polite**!!!

55

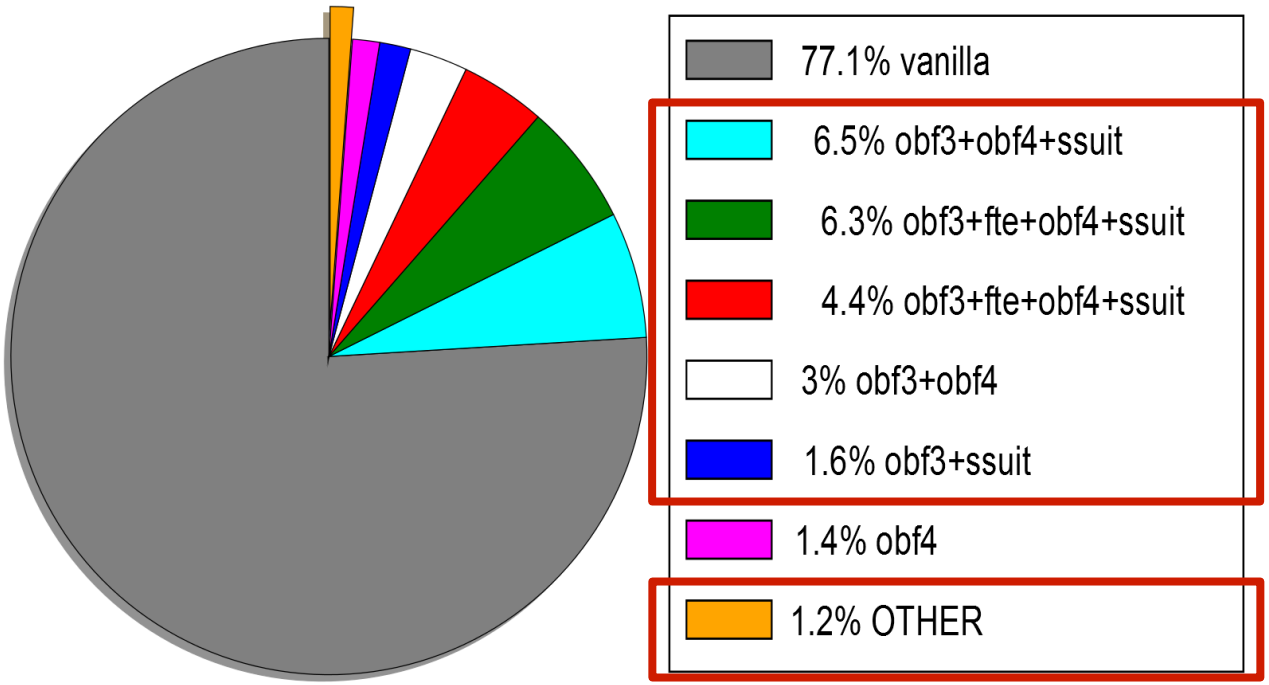
Bri

Bri

an)

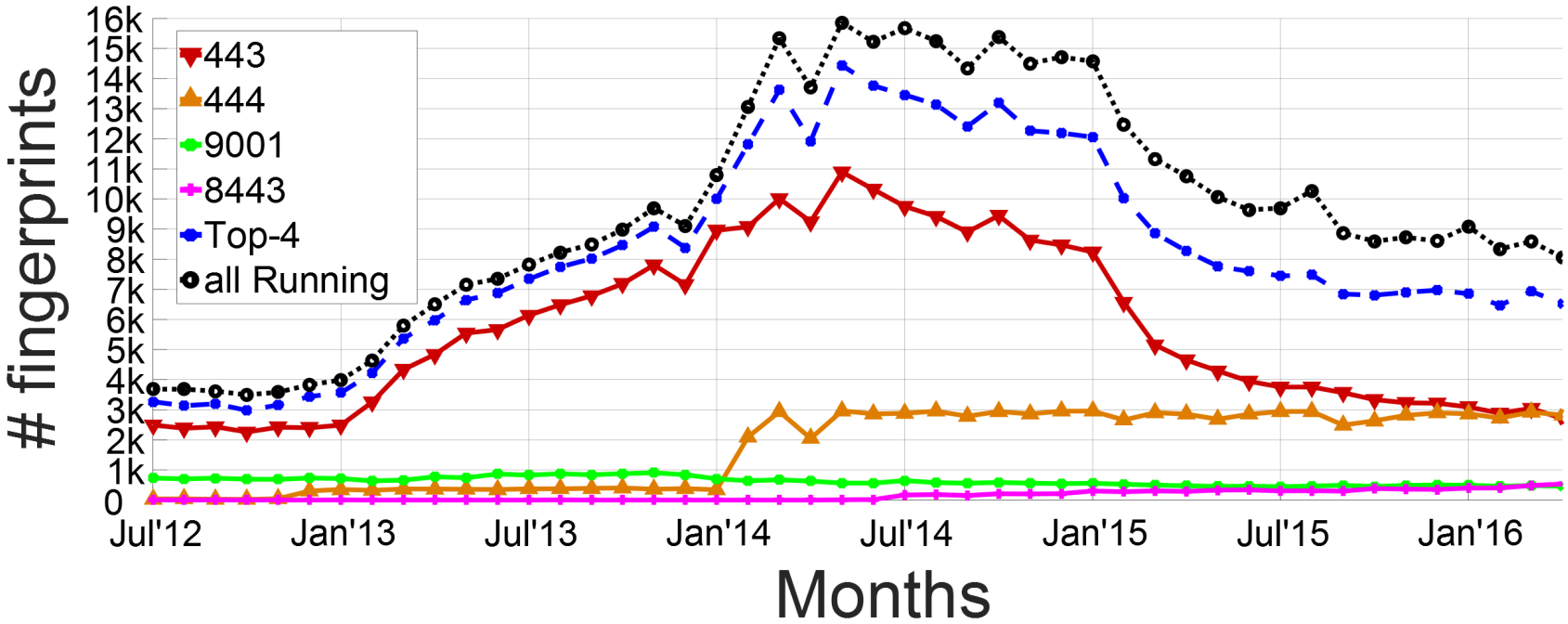
PT Deployment

April 2016



Conflicting security properties!

Or Port Distribution



Top-3 OR ports are used by 71% of public bridges

Scanning on those ports reveals majority of bridges!

Bridge Ranking

Not all bridges are equally important

How well is country-level blocking working?
How well is blocking of specific PT working?
Which bridges should censor target next?

CC	Used Brid.	Top 20 (Default)
cn	712	45.6% (44.0%)
ir	941	86.6% (86.1%)
sy	74	76.9% (68.0%)
uk	943	84.1% (84.0%)
us	1,496	58.7% (56.7%)
All	2,213	91.71% (91.4%)

91% traffic used default bridges!
Censor can disconnect users in reaction to an event

Outline

Intro

Approach

Public Bridge Analysis

Private Bridge Analysis

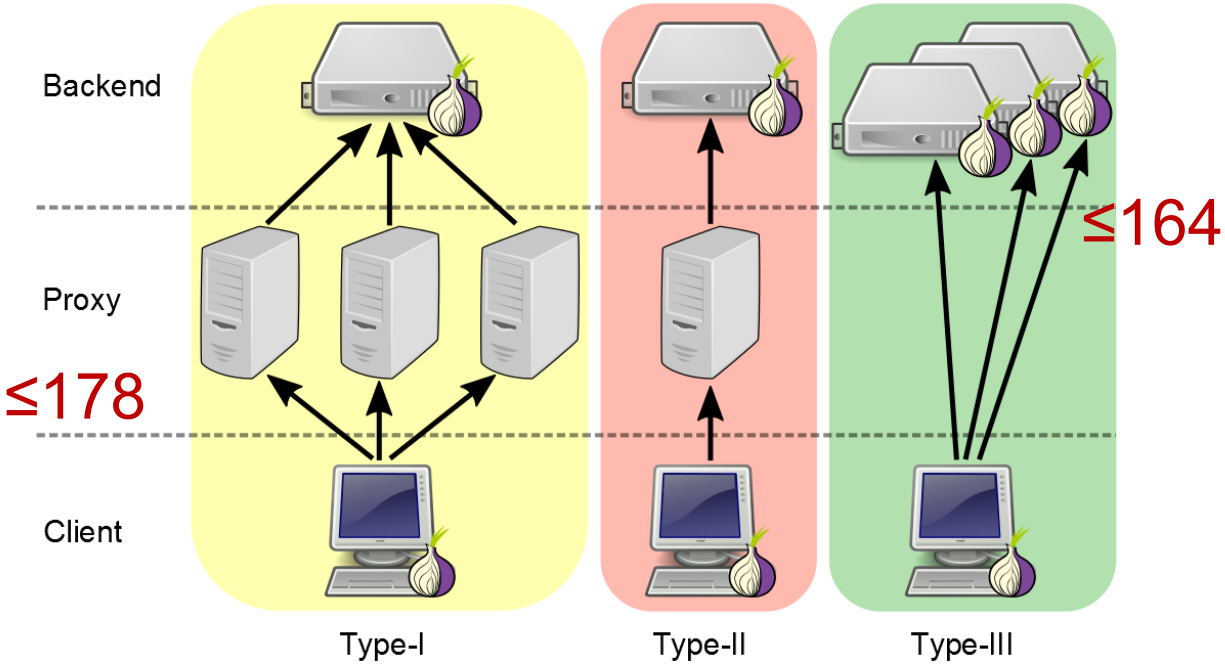
Bridge Discovery (April 2016)

Port	SC	Source	Disc.	Verified	Public	Private	Proxy
443	9	Censys	2,448	1,315 (1,122)	897 (860)	263 (262)	164
993	2	Censys	19	16 (13)	11 (11)	3 (2)	2
995	3	Censys	14	14 (13)	10 (10)	3 (3)	1
444	1	Shodan	14	12 (101)	8 (97)	1 (4)	4
8443	1	Shodan	191	156 (149)	148 (148)	1 (1)	7
9001	1	Shodan	2,001	1047 (587)	165 (166)	415 (421)	468
9002	1	Shodan	23	19 (5)	1 (1)	4 (4)	14
All	17	All	4,684	2,554 (1,986)	1,239 (1,292)	684 (694)	645

- Deanonymized 35% public bridges with clients
- Found 684 private bridges
- Found 645 private proxies
- 35% bridges private, 65% public

Bridge Cluster Types

1,343 clusters, 75% singletons



Type-I	: 47
Type-II	: 138
Type-III	: 88
Type-IV	: 43
Type-V	: 10
Mixed	: 16

77% Proxies and Backend in same AS
Proxies do not provide IP diversity

Conclusion

- Public Bridges
  - Bridges with clients live 4 months, no IP changes → Blocking
  - PTs with conflicting security properties
  - Top-3 OR ports 71% public bridges → Patch CollecTor
  - 91% bridge traffic uses default bridges → Defeats purpose
  - Bridge Ranking enables targeted attacks
- Bridge discovery
  - Deanonymized 35% of public bridges
  - Found 684 private bridges + 645 private proxies
  - 35% bridges are private
  - Clusters of bridges+proxies deployed → Little IP diversity
- Open OR Port needs fixing

institute imdea software

Questions?

www.software.imdea.org

Joint Work With

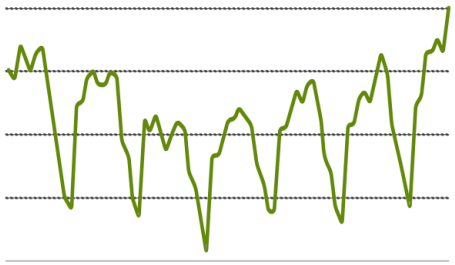
Srdjan Matic

Carmela Troncoso

Public Bridges Analysis

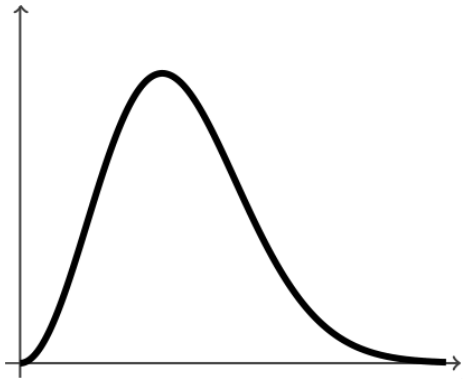
(1) Bridge Population

(2) Bridge Stability

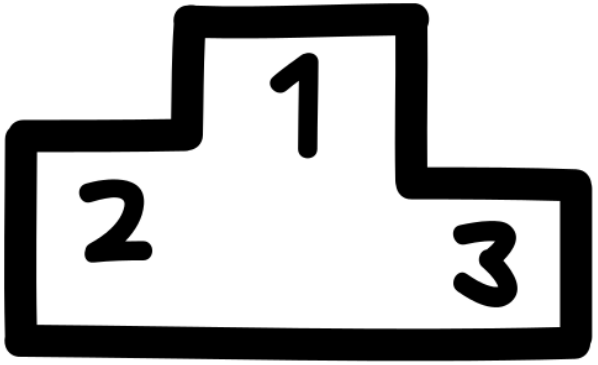


(3) PT Deployment

(4) OR Port Distribution



(5) Bridge Ranking



(6) CollecTor Security Analysis

COLLECTor

Private Bridge & Proxy Analysis

(1) Population

(2) Clusters

(3) Hosting

We first need to discover private bridges!

Cluster Types
Private Proxies

IP diversity
AS diversity

Bridge Clustering & Ranking

- Cluster bridges from same owners
  1. Same fingerprint
  2. Similar nicknames
  3. Same contact information
  4. Similar verified IP address
  5. Similar IP address in descriptor
- Rank Bridges
  - Not all bridges equally important

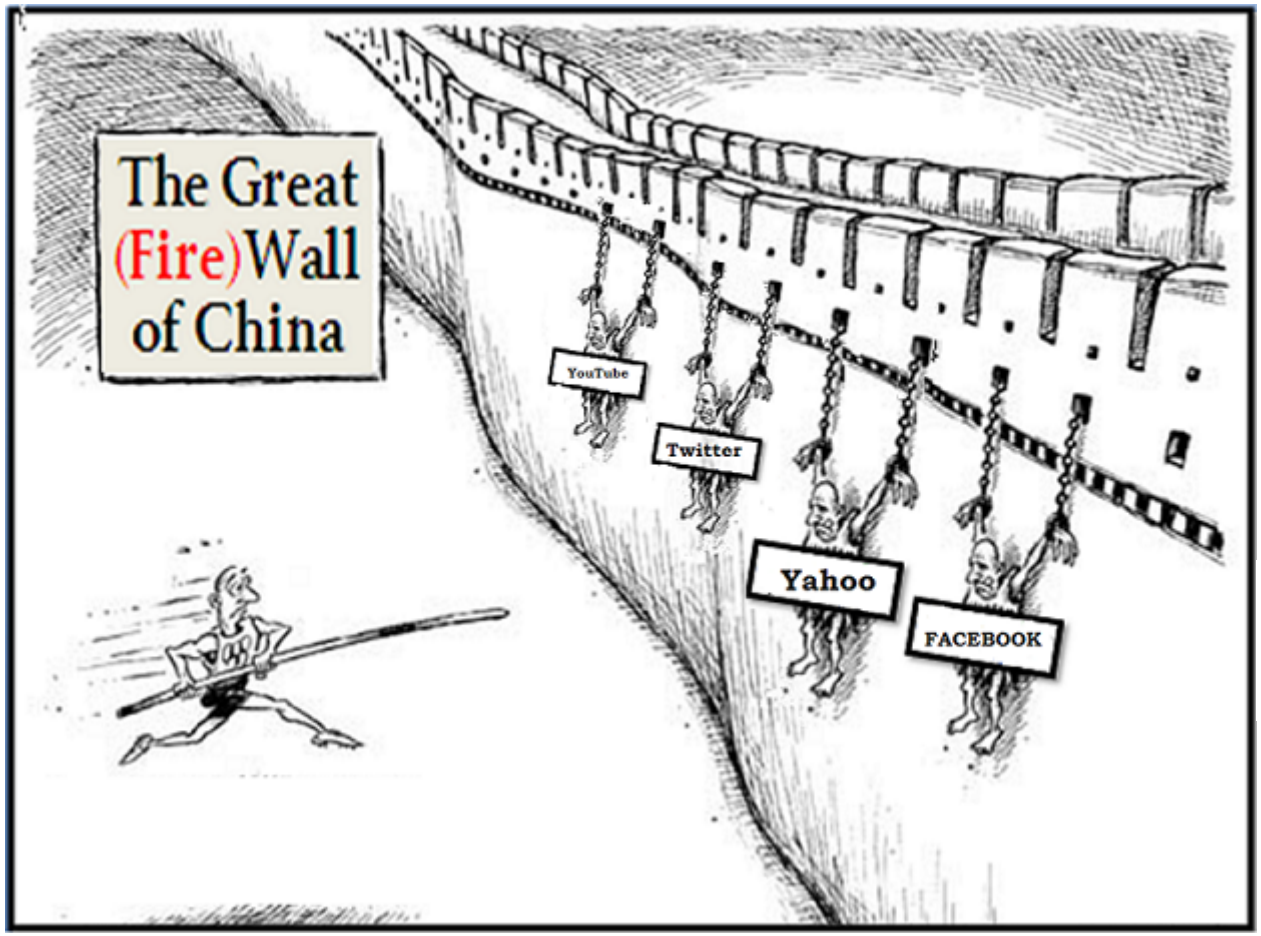
Related Work

- Design secure Pluggable Transports
  - Obfs4, Skypemorph, BridgeSPA, StegoTorus, ScrambleSuit
- Techniques to discover bridge IP
  - Ling et al., McLachlan and Hopper, Zmap

Ethical Considerations

- Approved by IMDEA's ethics review board
- Disclosed to Tor project at submission
- We only use leaks/info from public datasets
- No access to any user traffic
- No malicious Tor nodes added
- No deanonymized bridges revealed
- No data release

Internet Censorship



fingerprint
==
SHA1()