Protecting Users from Adversarial Networks

Roya Ensafi
University of Michigan

CNN World • TV CHANNELS

Destruction is seen in Borodianka, Ukraine, on April 5. Borodianka

an President Volodymyr Zelensky speaks to the media a

NEWS

The day the news died Here are all Russia's independent media outlets banned, blocked, or shuttered in just the past few days

12:49 am, March 5, 2022 · Source: Meduza

Russia blocks access to Facebook and Twitter

Russian Internet Takes a Hit as Cogent Cuts Off Its Backbone Network

A major internet service provider's disconnection is a new step toward the "splinternet" that adds fragmentation to the global communication network.

WIRED BACKCHANNEL BUSINESS CULTURE GEAR IDEAS SCIENCE SECURITY SIGN IN SUBSC

Russia's Internet Censorship Machine Is Going After Tor

The attempt to block the site, which helps users mask their online activity, is the latest in the country's efforts to control the internet.

Over 600 Companies Have Withdrawn from Russia—But Some Remain

April 14, 2022

Russia is blocking more and more VPNs

By Anthony Spadafora published 23 days ago

BBC, CNN and other global news outlets suspend reporting in Russia

BBC's director-general says new Russian legislation 'appears to criminalise the process of independent journalism'

TikTok created an alternate universe just for Russia

The Chinese-owned social media giant weathered Putin's information crackdown by muzzling its users there and cutting them off from the outside world, while allowing state propaganda


#MahsaAmini
مهسا امینی


POLICE
POLICE
POLICE
POLICE

Technical questions:

- What **sites** are being blocked? What is still accessible?
- How, technically, has Russia implemented its **information controls**?
- What will Russia likely do next ?
- What does this mean for **Internet freedom** ?

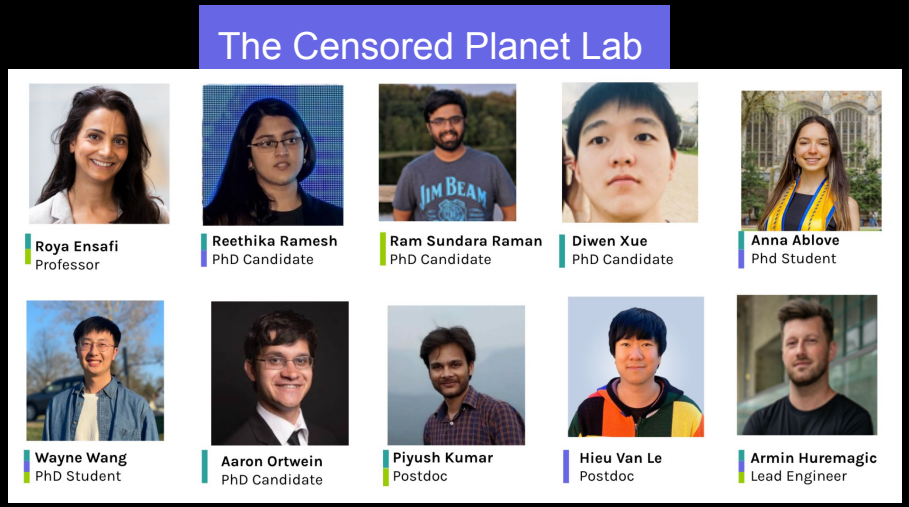
Detecting and defending against adversarial networks is challenging, due to the **Internet's vast size and heterogeneity**, **the powerful capabilities of in-network threat actors**, and **the lack of ground-truth**.

Experiments must be conducted ethically and safely.

I build scalable techniques and systems to protect users from adversarial networks that violate the **confidentiality, integrity,** or **availability** of users' legitimate traffic.

WHO	WHAT
Governments	Blocking
Consumer ISPs	Tampering
VPNs	Net neutrality violation
Transit ISPs	Mass surveillance
Cellular providers	Targeted surveillance
Content providers	Content removal
Content delivery networks	Throttling
Device manufacturers	Denial of Service (DoS)
Hackers for hire	

My team build scalable techniques and systems to protect users from adversarial networks that violate the **confidentiality, integrity,** or **availability** of users' legitimate traffic.



In this talk, I cover…

Leveraging side channel measurement to **detect and understand censorship**

Applying a multi-perspective approach to **safeguard the consumer VPN ecosystem**

Investigating the **Geo-inequity** of users' online experiences

Detecting Censorship with Side Channels

The Art of Censorship Analysis
FOCI 2023

Censored Planet: An Internet-wide, Longitudinal Censorship Observatory
ACM CCS 2020

Measuring the Deployment of Network Censorship Filters at Global Scale;
NDSS 2020

Quack: Scalable Remote Measurement of Application-Layer Censorship
USENIX Security 2018

Internet-Wide Detection of Connectivity Disruptions
IEEE S&P (“Oakland”) 2017
Invited to appear in the IEEE Security & Privacy Magazine

Global Measurement of DNS Manipulation
USENIX Security 2017
Invited to appear in USENIX ;login:, Winter 2017 Issue

Analyzing the Great Firewall of China Over Space and Time
PETs 2015

Detecting Intentional Packet Drops on the Internet via TCP/IP Side Channels
Passive and Active Measurement (PAM), 2014

Idle Scanning and Non-interference Analysis of Network Protocol Stacks Using Model Checking
USENIX Security 2010

How Have We Collected Data on Censorship?

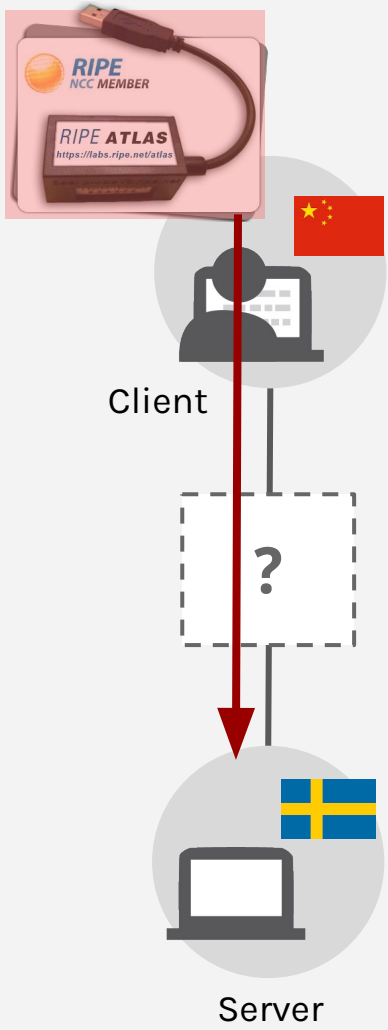
Old state of the art:

- Deploy hardware or software in censored region (e.g. RIPE Atlas, OONI probe)
- Ask people on the ground, or use VPNs, or research networks (e.g., PlanetLab)

THREE KEY CHALLENGES:

Coverage, continuity, and ethics

Collecting consistent, continuous, and global data requires a different approach.

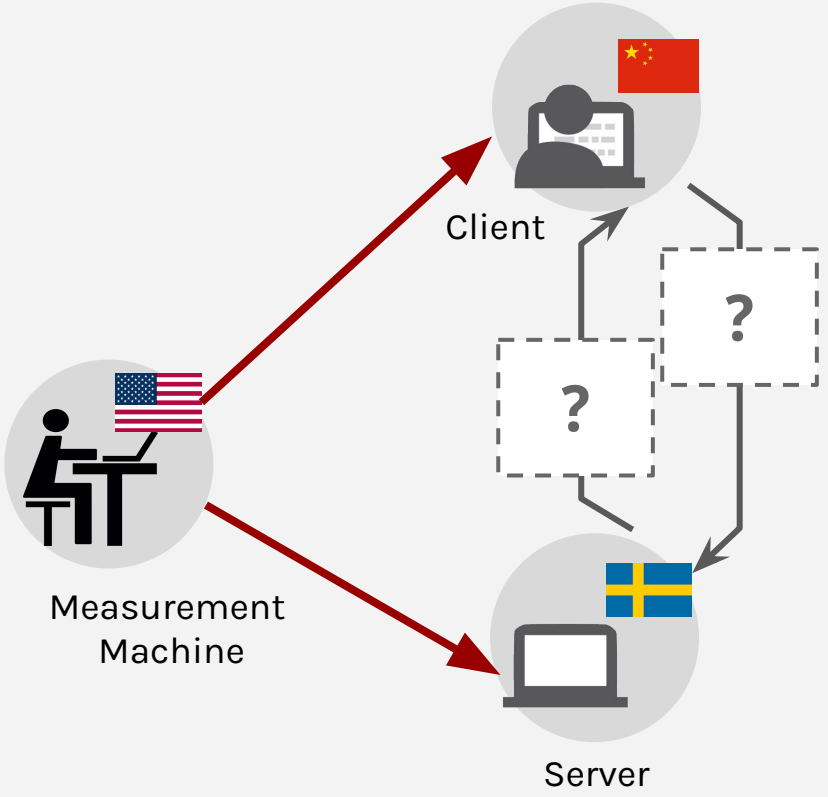


Measuring Internet Censorship Globally… Remotely!

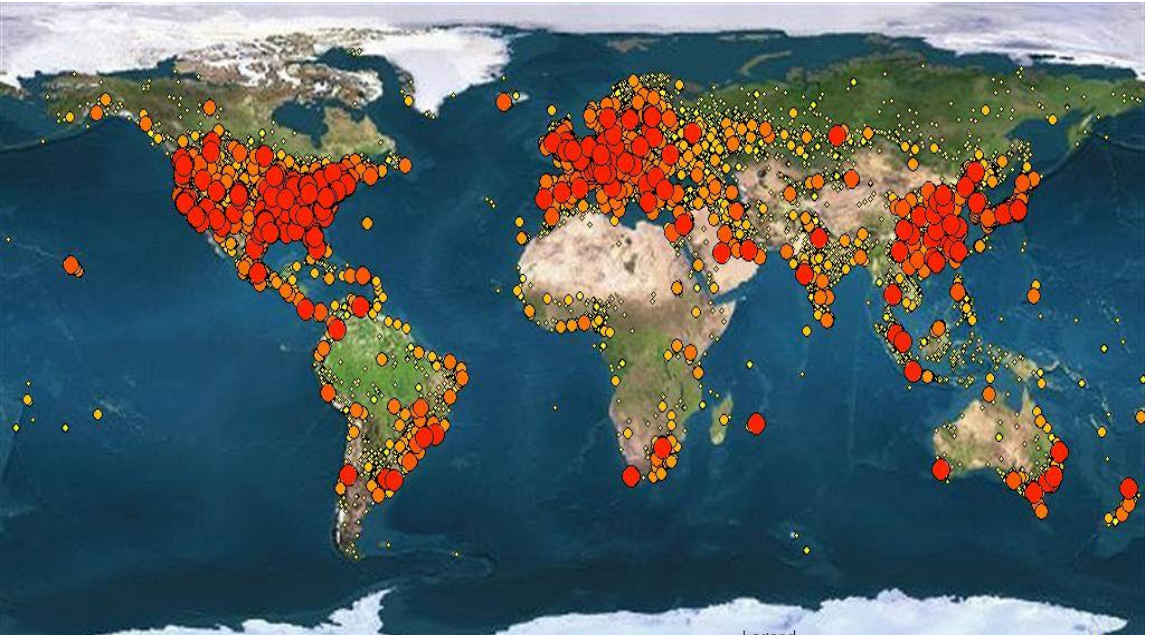
REFRAMING THE PROBLEM:

How can we detect whether pairs of hosts around the world can talk to each other?

… without volunteer participation?



Leveraging Existing Hosts as Vantage Points



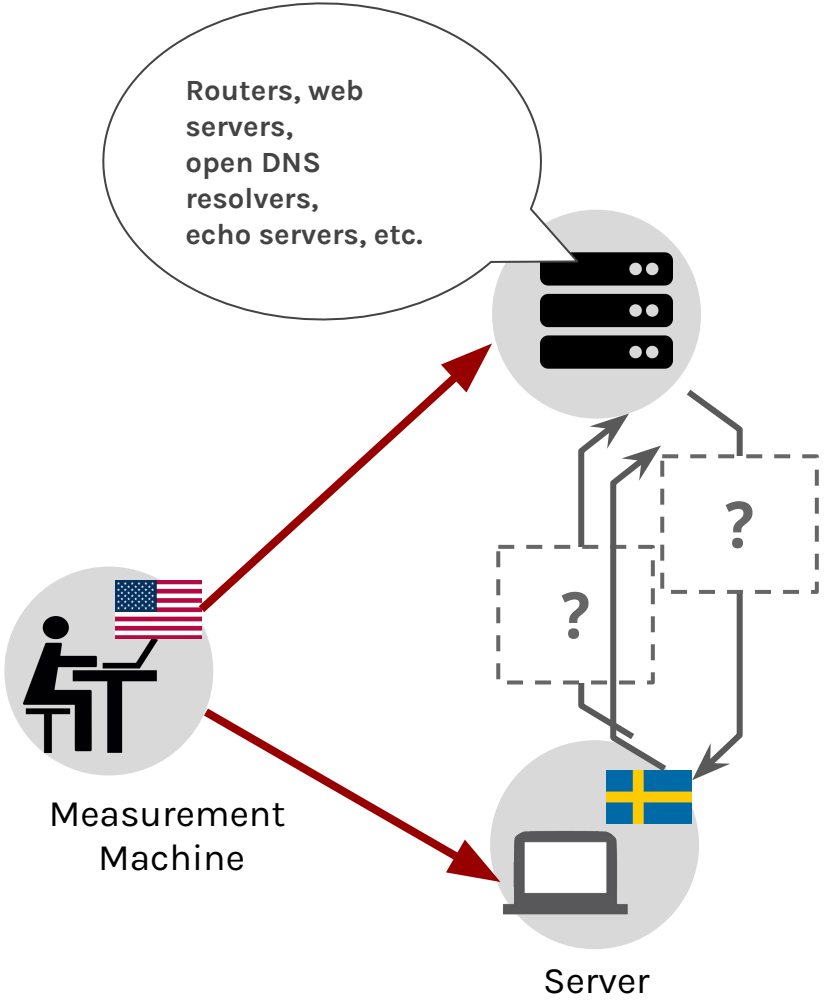
217 million IPv4 hosts w/ open ports
7 million open DNS resolvers
2 billion web servers
…

These machines speak to the world, and they follow **different Internet Protocols.**

My Approach:
Using Side Channels

REFRAMING THE PROBLEM:

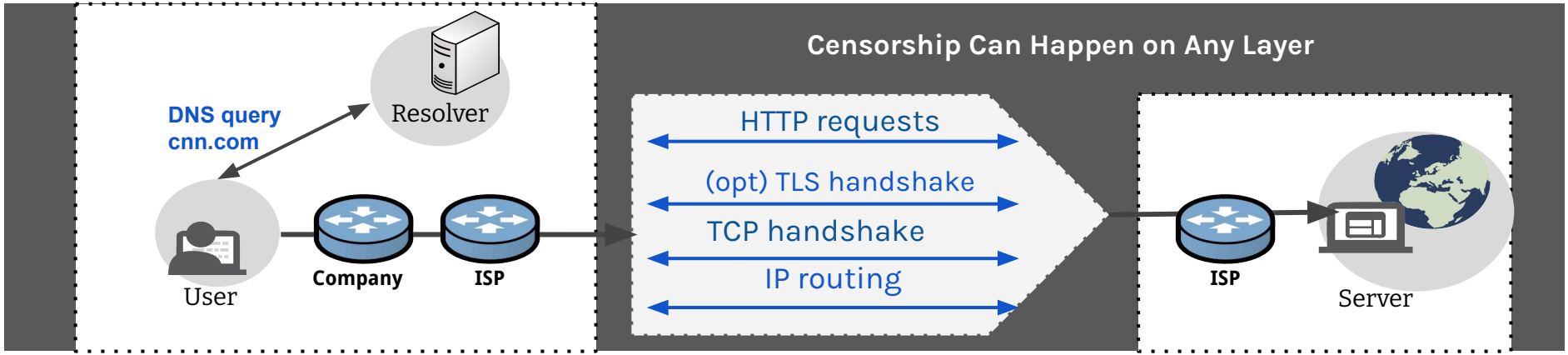
How can we leverage
subtle behavior of different Internet Protocols
to detect whether two distant hosts can
communicate on a given layer?



Side Channels Techniques for Remotely Measuring Censorship

DNS Layer	TCP/IP Layer	Application Layer
Satellite (2017) → Institutional open resolvers	**Spooky (2014)** **Augur (2017)** → Global IP_ID routers	**Quack (2018)** **HyperQuack (2020)** → Services that reflect data (e.g. Echo, HTTP, HTTPS)

Side Channels Techniques for Remotely Measuring Censorship



DNS Layer

Satellite (2017) →
Institutional open resolvers

TCP/IP Layer

Spooky (2014)
Augur (2017)
→ Global IP_ID routers

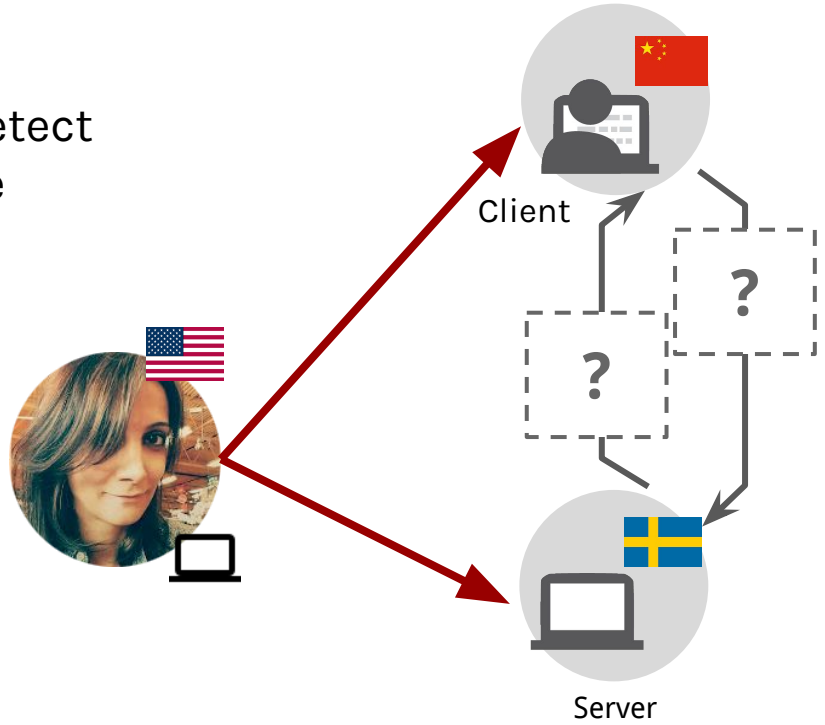
Application Layer

Quack (2018)
HyperQuack (2020)
→ Services that reflect data (e.g. Echo, HTTP, HTTPS)

Spooky Scan

Spooky Scan uses TCP/IP side-channels to detect whether a client and server can communicate (and in which direction packets are blocked)

Goal: Detect blocking from off-path



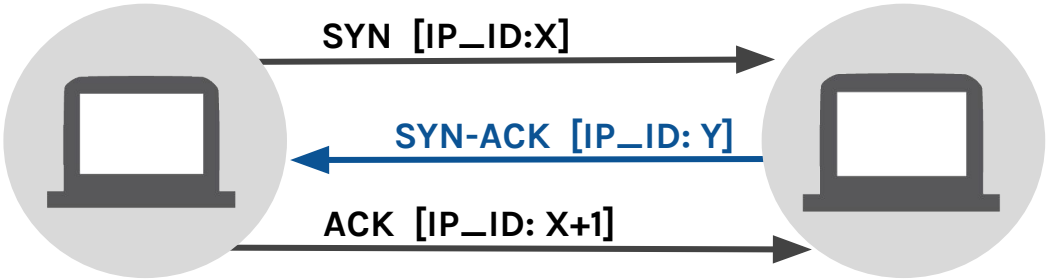
* **Detecting Intentional Packet Drops on the Internet via TCP/IP Side Channels**
  Roya Ensafi, Knockel, Alexander, and Crandall (PAM '14)

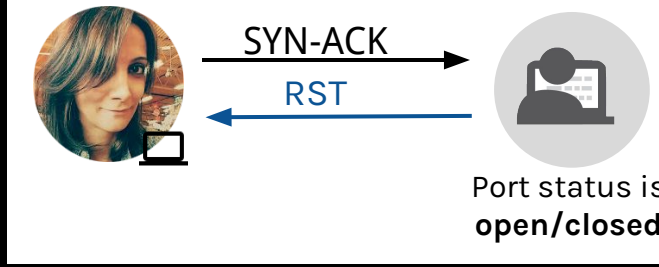
* **Idle Port Scanning and Non-interference Analysis of Network Protocol Stacks Using Model Checking**
  Roya Ensafi, Park, Kapur, and Crandall (Usenix Security 2010)

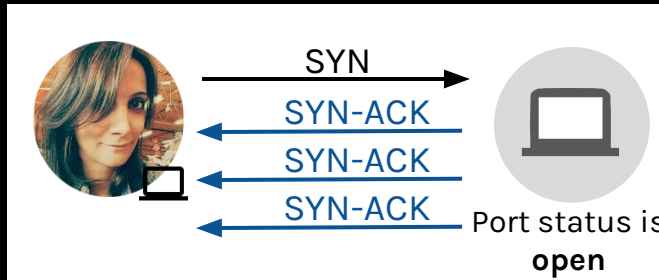
* **TCP Idle Scan** Antirez (Bugtraq 1998)

Background: TCP/IP Protocol

TCP Handshake:







Spooky Scan Requirements

Client

Must maintain a global value for IP_ID

Server

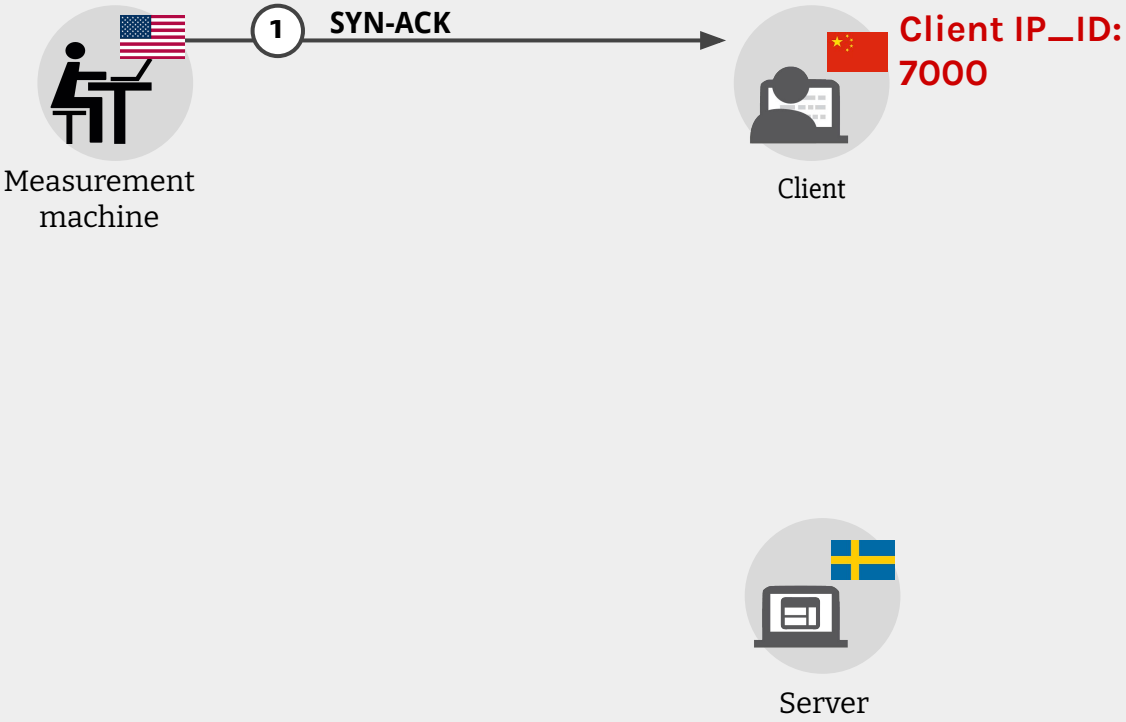
Open port and retransmitting SYN-ACKs

Measurement Machine

Must be able to spoof packets

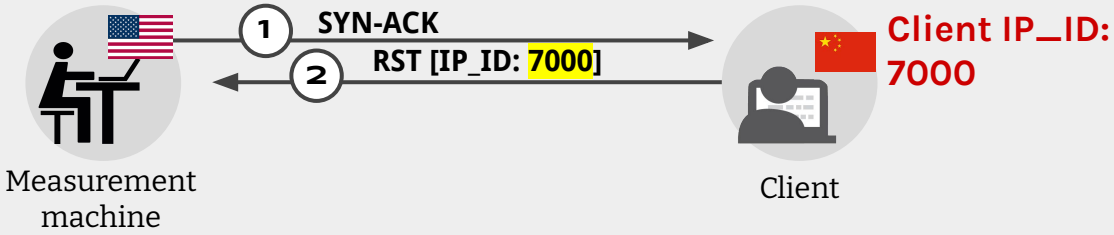
Spooky Scan

No direction blocked



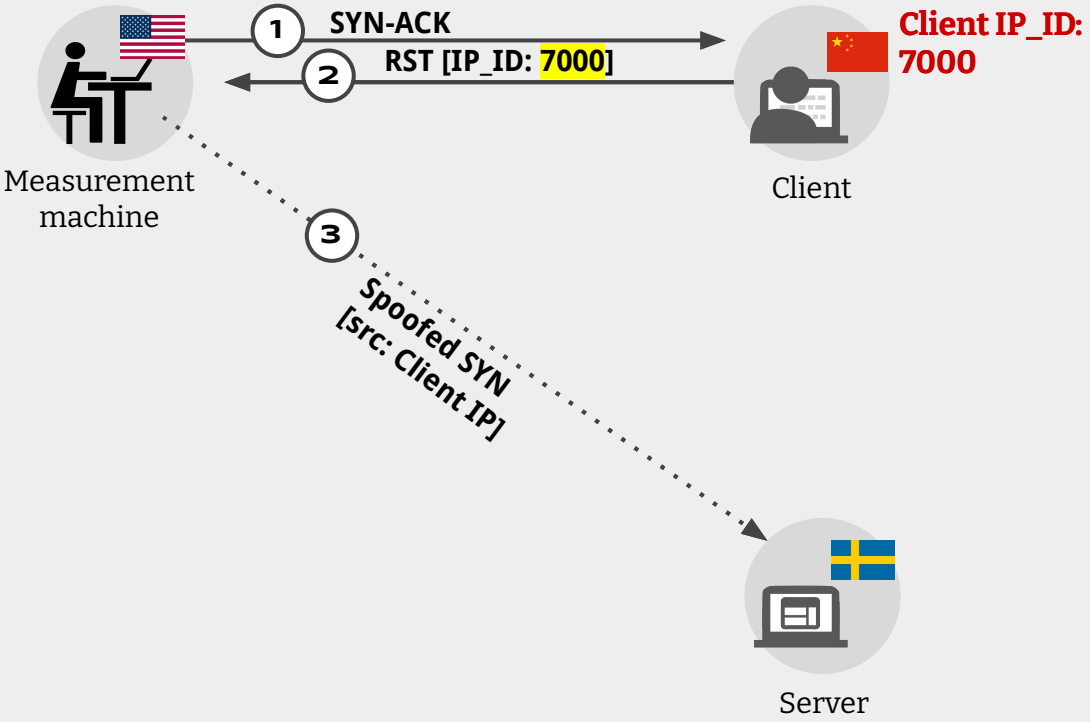
Spooky Scan

No direction blocked



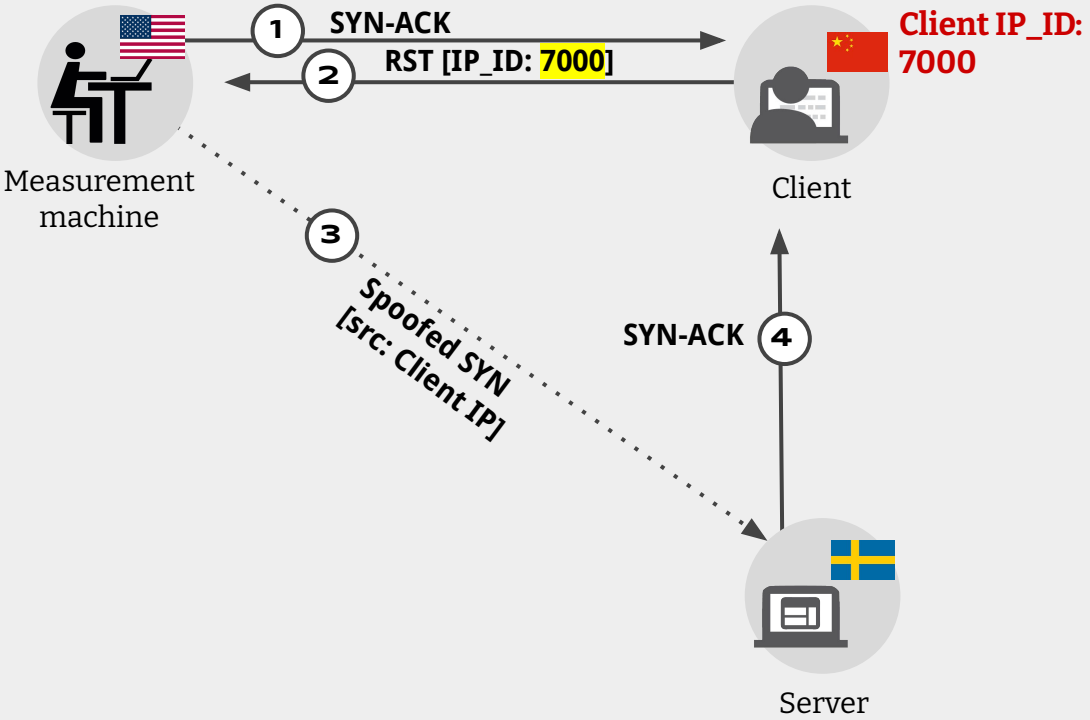
Spooky Scan

No direction blocked



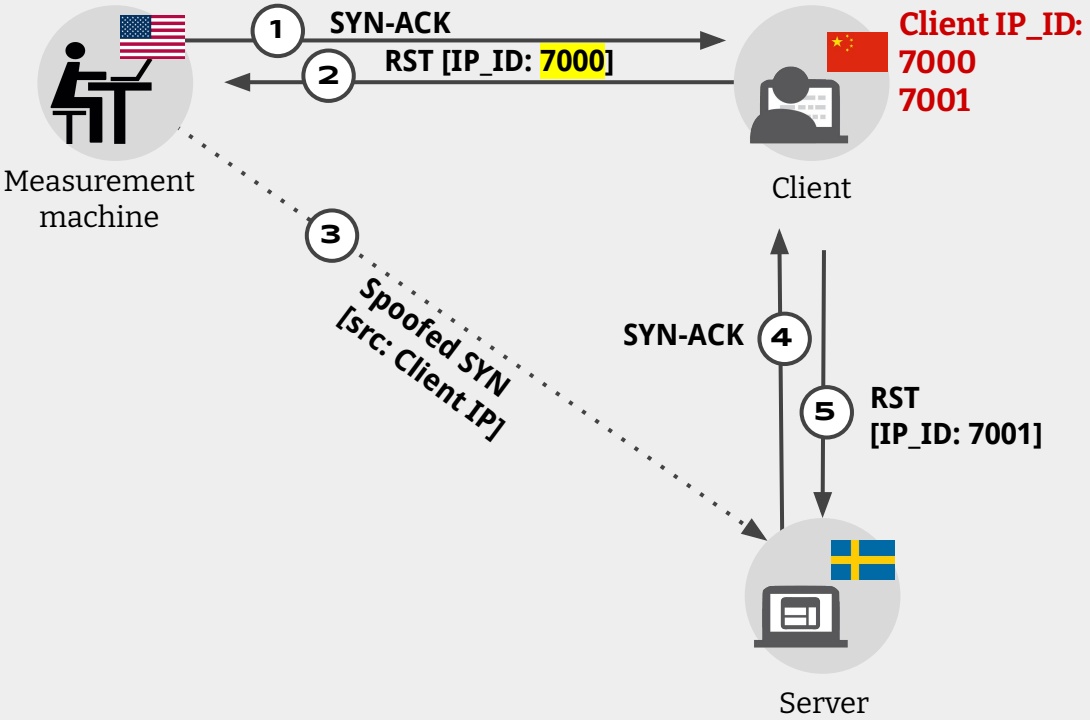
Spooky Scan

No direction blocked



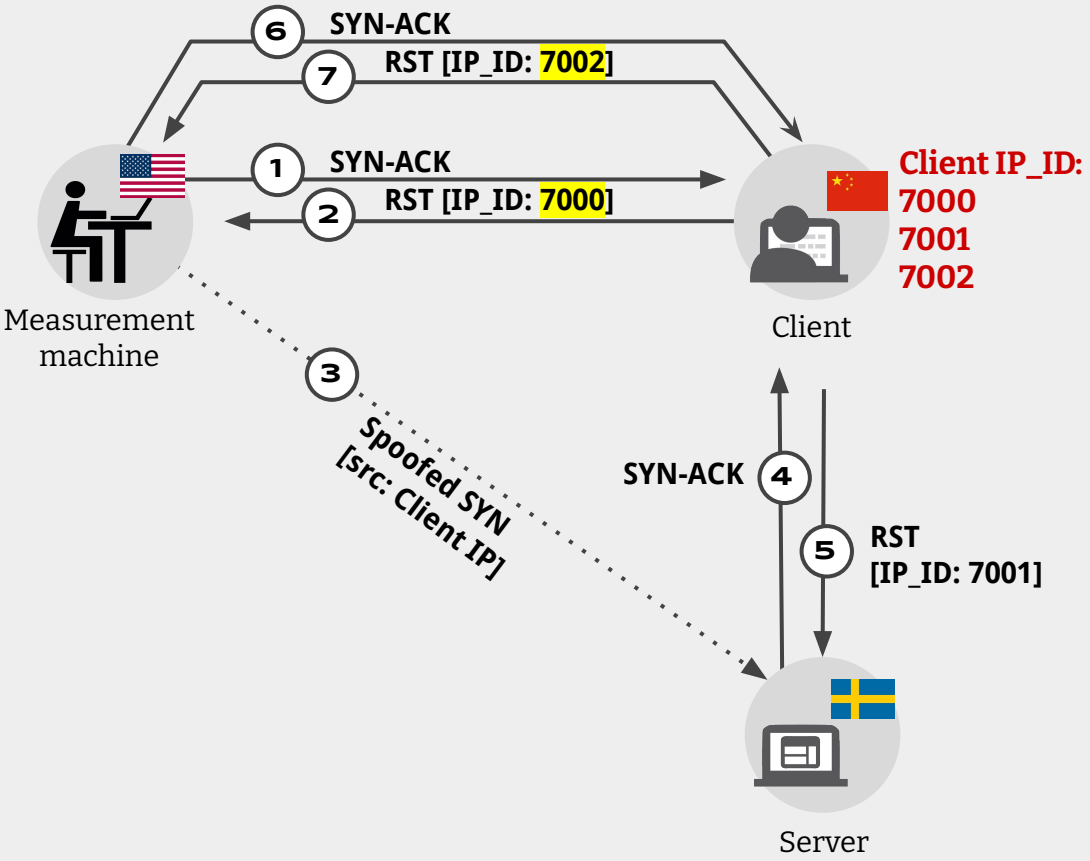
Spooky Scan

No direction blocked



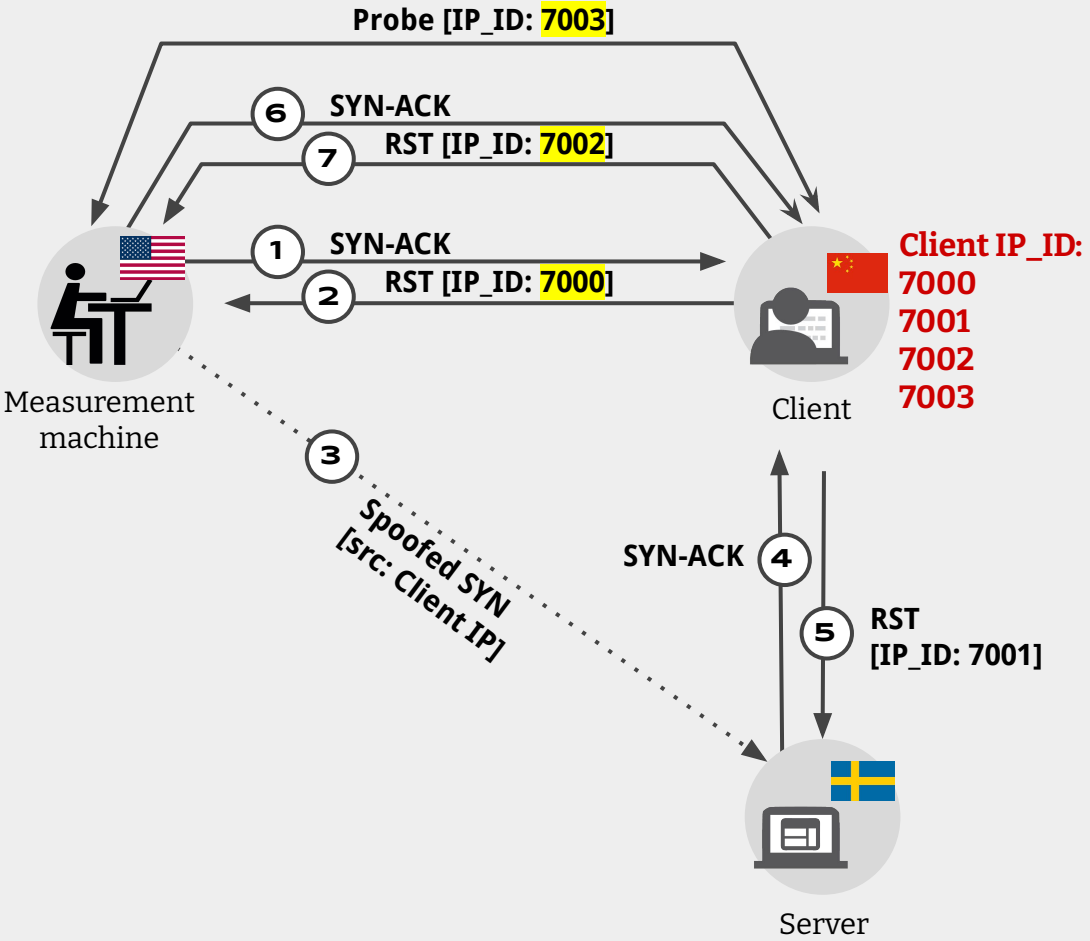
Spooky Scan

No direction blocked



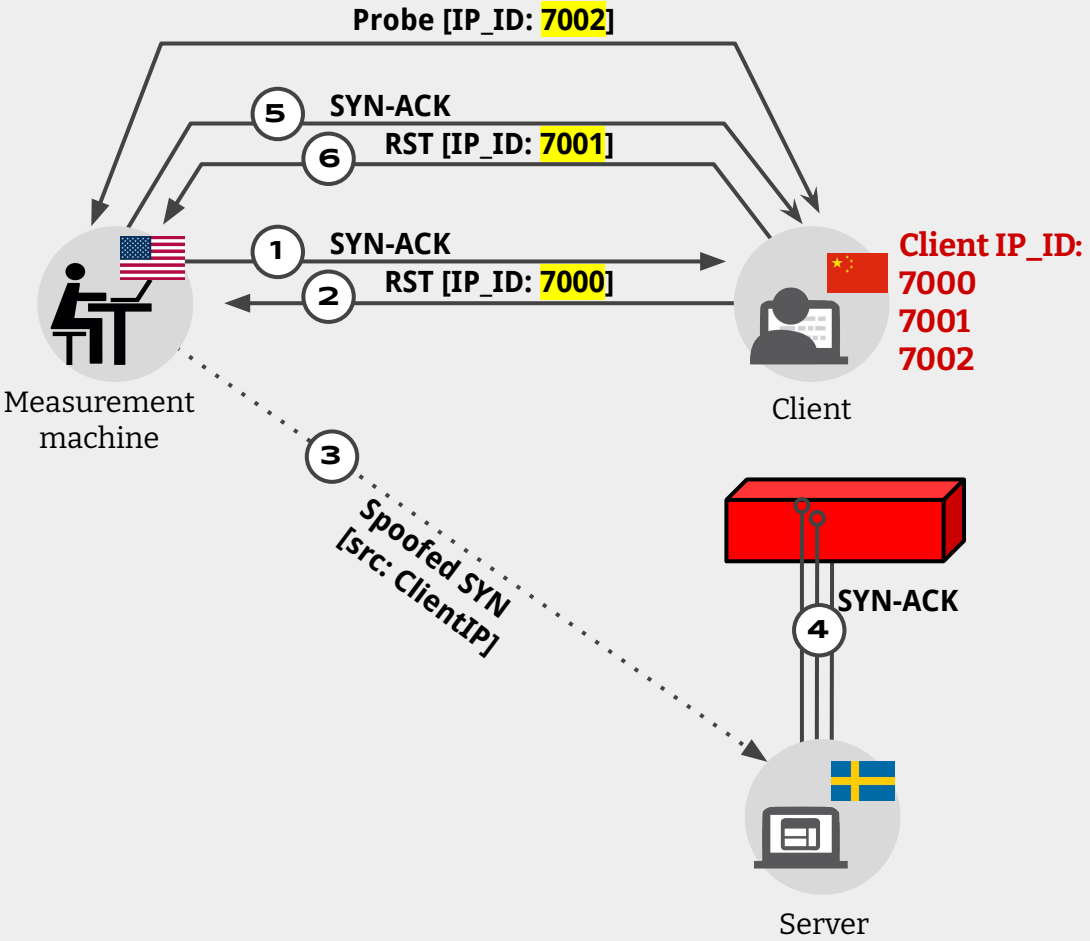
Spooky Scan

No direction blocked



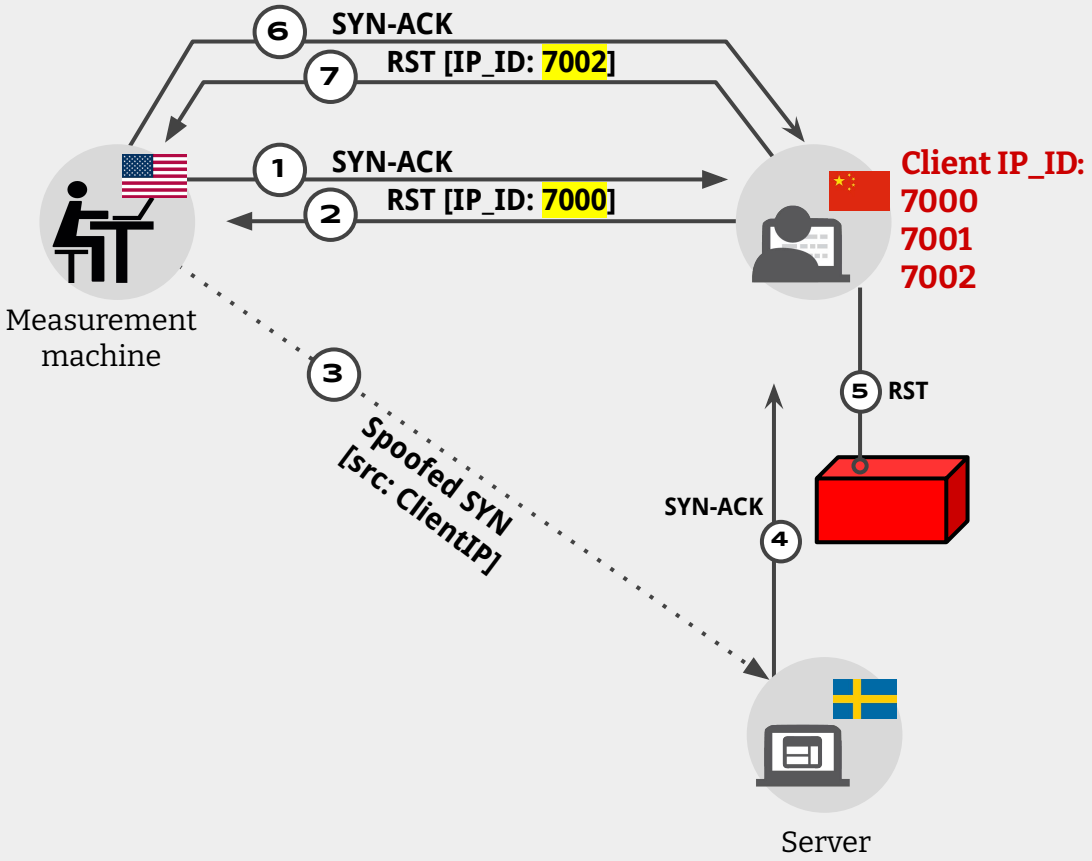
Spooky Scan

Server-to-Client blocked



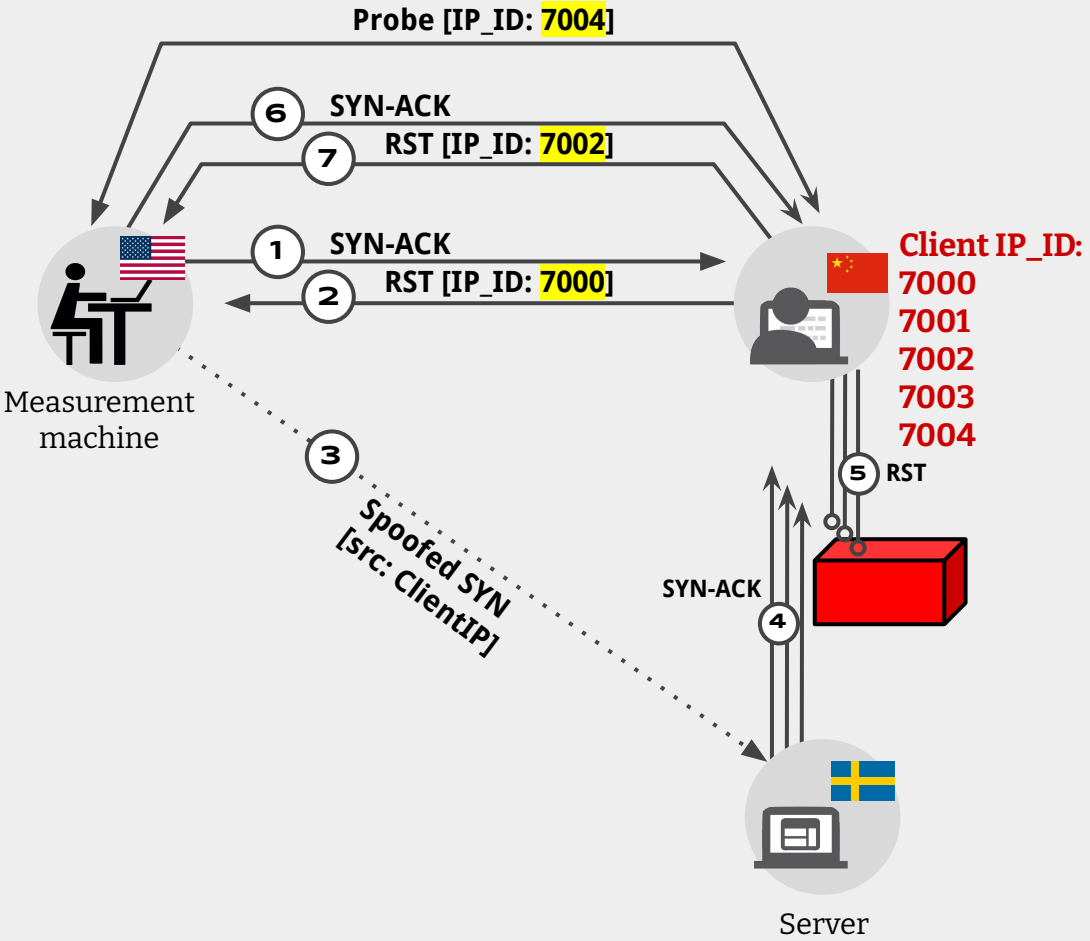
Spooky Scan

Client-to-Server blocked



Spooky Scan

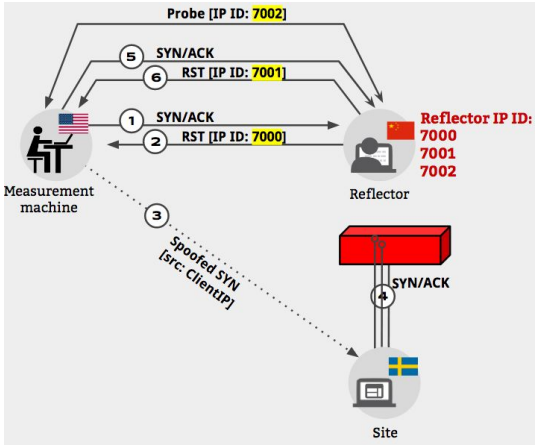
Client-to-Server blocked



Spooky Scan

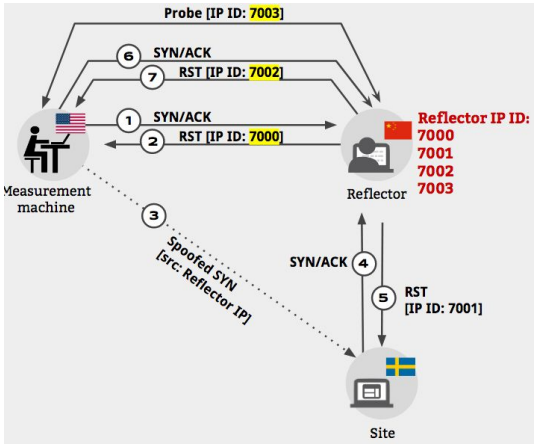
Server-to-Client Blocked

Δ IP_ID1 = 1
Δ IP_ID2 = 1



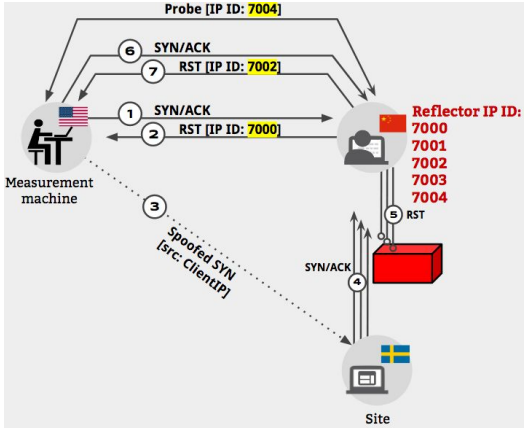
No Direction Blocked

Δ IP_ID1 = 2
Δ IP_ID2 = 1

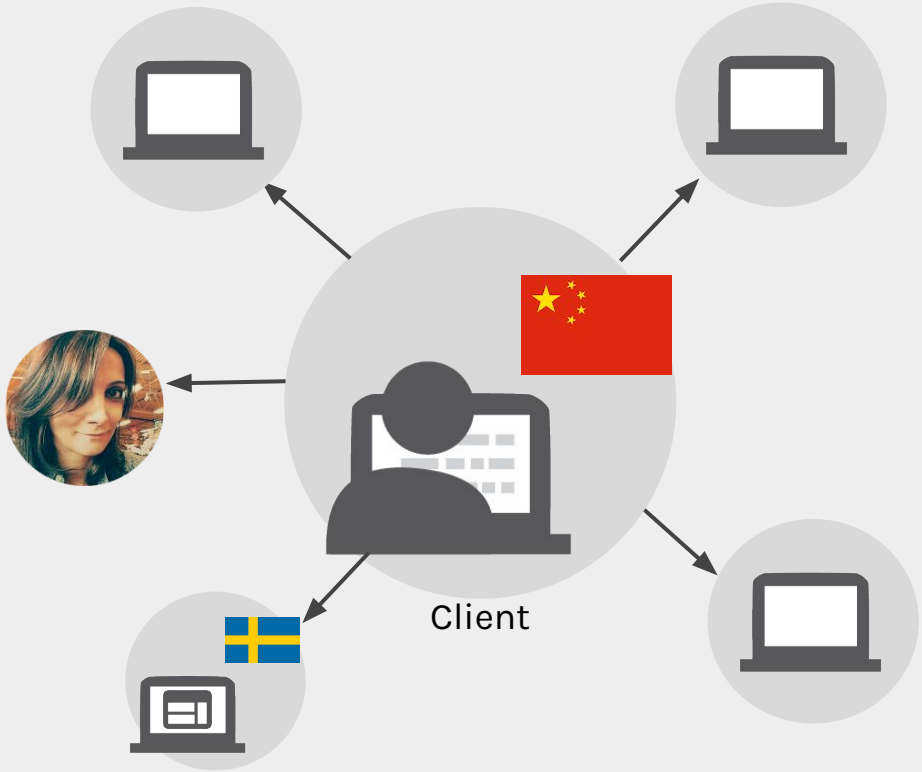


Client-to-Server Blocked

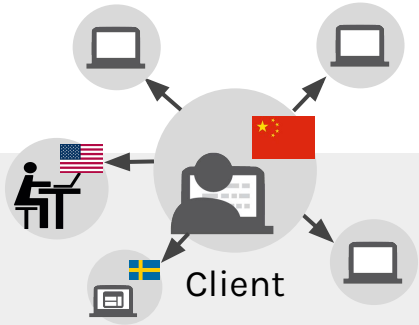
Δ IP_ID1 = 2
Δ IP_ID2 = 2



Client IP_ID Noise



Coping with Client IP_ID Noise

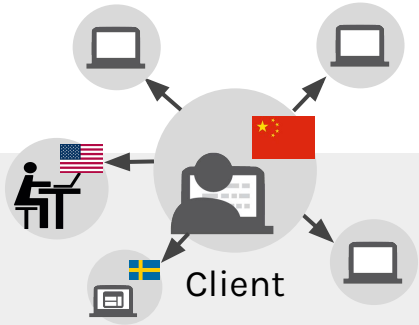


Amplifying the signal

Effect of sending *N* spoofed SYNs:

Server-to-Client Blocked	No Direction Blocked	Client-to-Server Blocked
Δ IP_ID1 = (1 + noise) Δ IP_ID2 = noise	Δ IP_ID1 = (1 + N + noise) Δ IP_ID2 = noise	Δ IP_ID1 = (1 + N + noise) Δ IP_ID2 = (1 + N + noise)

Coping with Client IP_ID Noise



Amplifying the signal

Effect of sending *N* spoofed SYNs:

Server-to-Client Blocked	No Direction Blocked	Client-to-Server Blocked
Δ IP_ID1 = (1 + noise) Δ IP_ID2 = noise	Δ IP_ID1 = (1 + N + noise) Δ IP_ID2 = noise	Δ IP_ID1 = (1 + N + noise) Δ IP_ID2 = (1 + N + noise)

Repeating the experiment

To eliminate the effects of packet loss, sudden bursts of packets, ...

Spooky Scan with Noise: Visualization

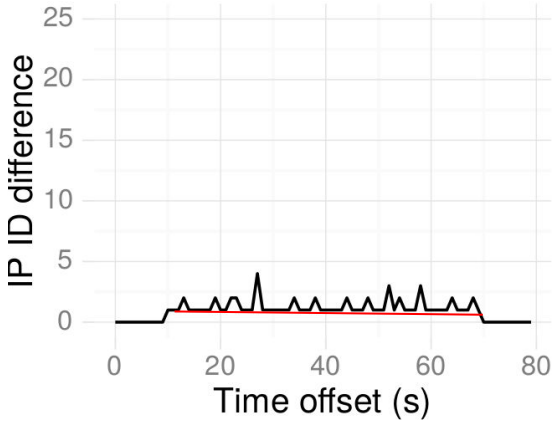
Probing method

For first 30s, query IP_IDs. Then, for another 30s

- Send 5 spoofed SYNs per second
- Query IP_ID once per second

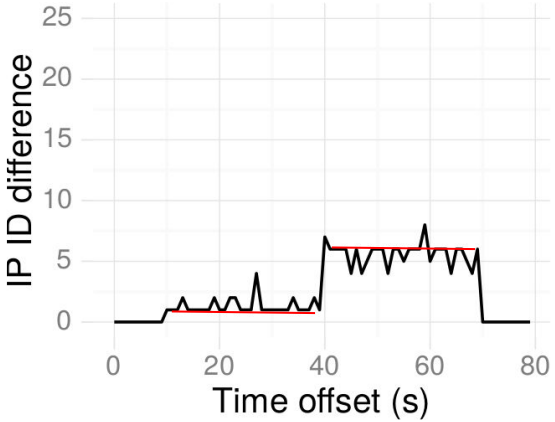
Server-to-Client Blocked

Tor relay (SE) to client (CN) blocked



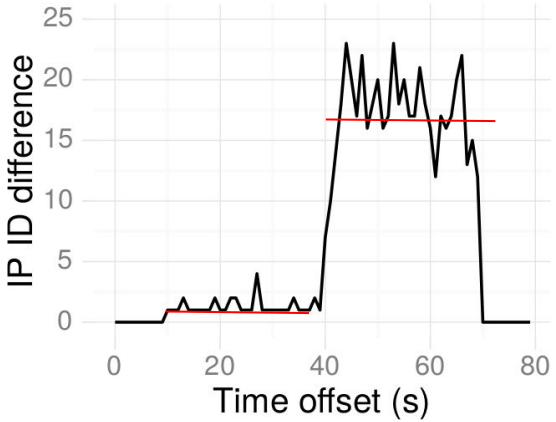
No Direction Blocked

No block btw client (US) and Tor relay (SE)



Client-to-Server Blocked

Client (AZ) to Tor relay (SE) blocked



Augur: Spooky for Continuous Scanning

PROBLEM: Want to optimize Spooky to probe many hosts, all the time.

INSIGHT: Some measurements are much noisier than others.

Augur: Spooky for Continuous Scanning

PROBLEM: Want to optimize Spooky to probe many hosts, all the time.

INSIGHT: Some measurements are much noisier than others.

Probing Methodology:

Until we have high enough confidence (or up to):

Run
- For first 4s, query IP_ID every sec
- Send 10 spoofed SYNs
  Query IP_ID
- Query IP_ID

Augur: Spooky for Continuous Scanning

PROBLEM: Want to optimize Spooky to probe many hosts, all the time.

INSIGHT: Some measurements are much noisier than others.

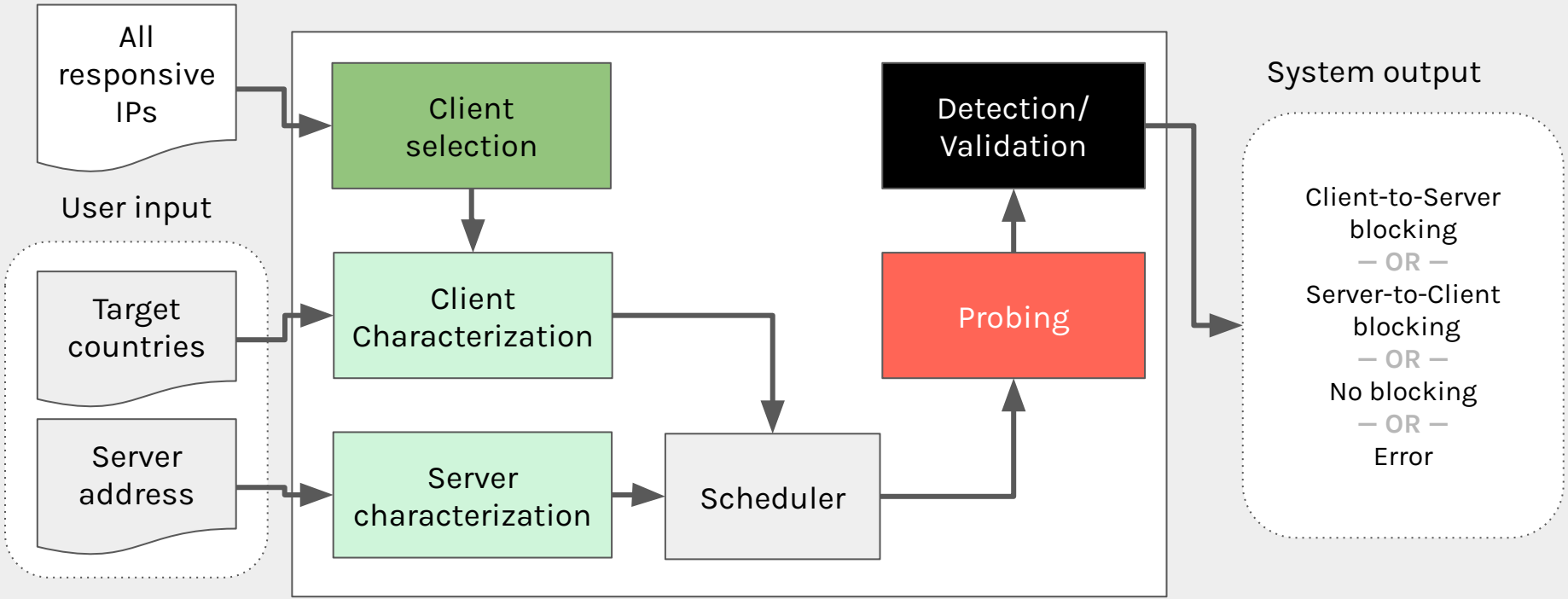
Probing Methodology:

Until we have high enough confidence (or up to):

Run
- For first 4s, query IP_ID every sec
- Send 10 spoofed SYNs
  Query IP_ID
- Query IP_ID

Repeat runs and use Sequential Hypothesis Testing to gradually build confidence.

Augur Framework



Coverage

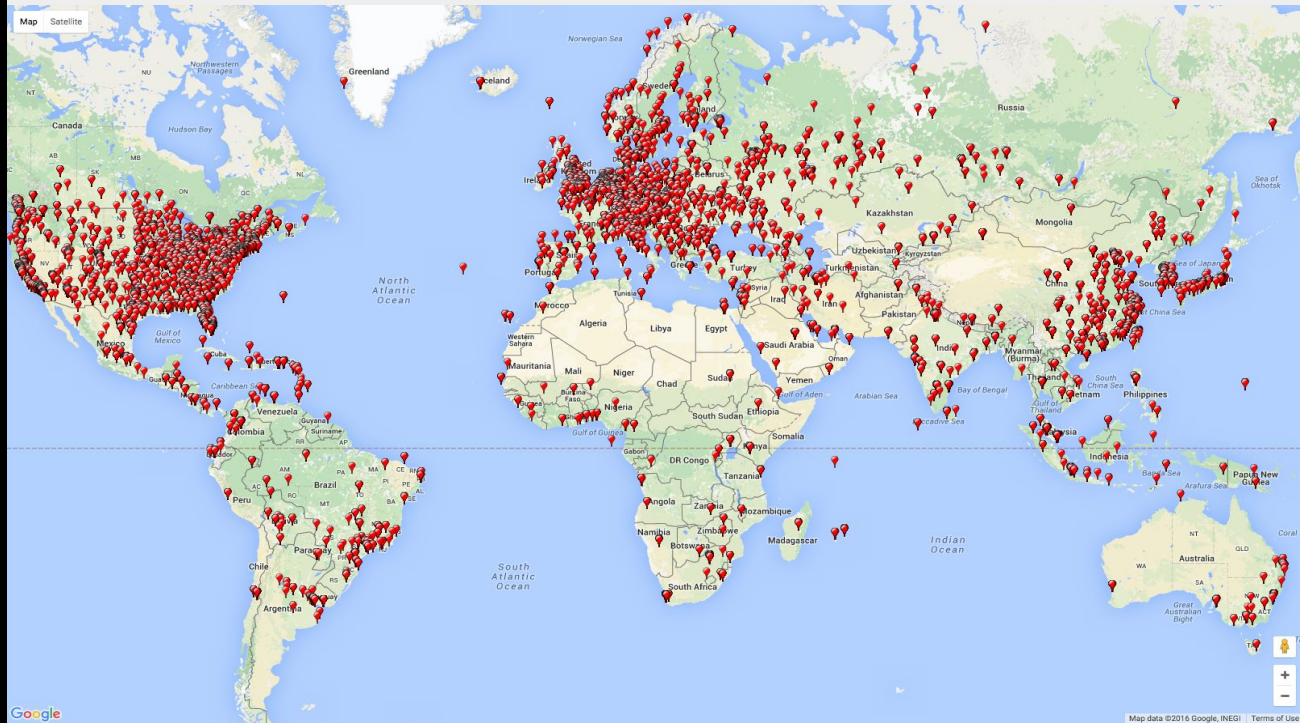
Scanning IPv4 on port 80:

22.7 million potential clients (with global IP_ID)

Compare: 10,000 in prior work (RIPE Atlas)

CHALLENGE:

Need global vantage points from which to measure



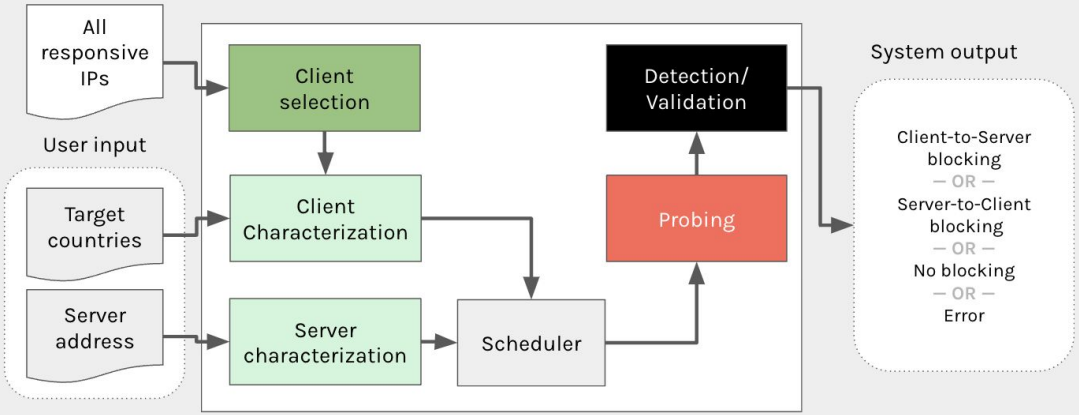
THREE KEY CHALLENGES:
Coverage, continuity, and ethics

Continuity

CHALLENGE:

Need to repeat measurements over time

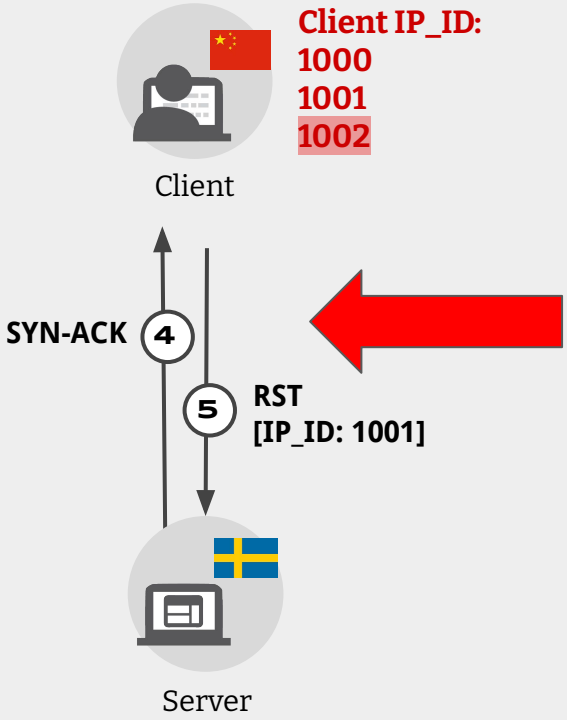
Augur doesn't depend on end users' participation, allowing us to collect measurements continuously.



Ethics

CHALLENGE:

Probing banned sites from users' machines creates risk



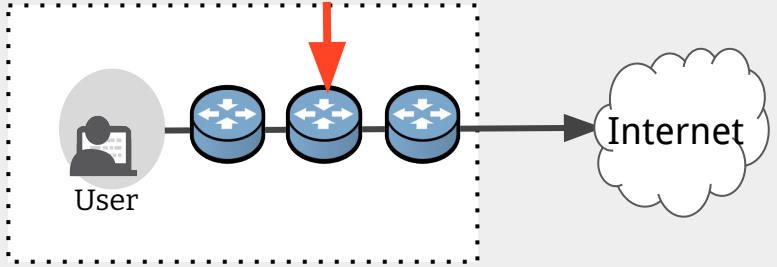
Ethics

CHALLENGE:

Probing banned sites from users' machines creates risk

THREE KEY CHALLENGES:
Coverage, continuity, and ethics

Use only **infrastructure devices** to source probes

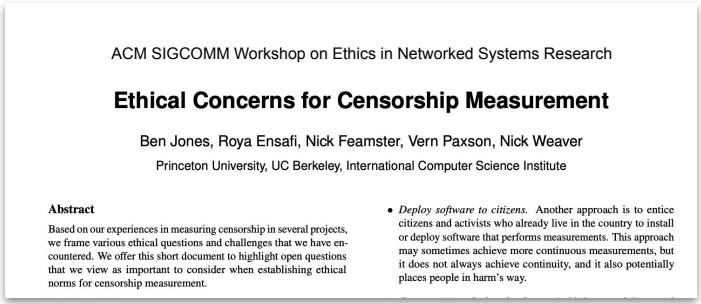


Global IP_ID	22.7 million	236 countries (and dependent territories)
Two hops back from end user	53,000	**180 countries**

Ethics in Censorship Measurement

More generally, censorship research frequently raises ethical considerations.

E.g., under what conditions is it safe enough to use remote vantage points?



ACM SIGCOMM Workshop on Ethics in Networked Systems Research

Ethical Concerns for Censorship Measurement

Ben Jones, Roya Ensafi, Nick Feamster, Vern Paxson, Nick Weaver

Princeton University, UC Berkeley, International Computer Science Institute

Abstract

Based on our experiences in measuring censorship in several projects, we frame various ethical questions and challenges that we have encountered. We offer this short document to highlight open questions that we view as important to consider when establishing ethical norms for censorship measurement.

- *Deploy software to citizens.* Another approach is to entice citizens and activists who already live in the country to install or deploy software that performs measurements. This approach may sometimes achieve more continuous measurements, but it does not always achieve continuity, and it also potentially places people in harm's way.

IRBs are often not positioned to help.

> Common Rule (45 CFR 46.102(f)) defines a human subject as "a living individual about whom an investigator conducting research obtains (1) data through intervention or interaction with the individual or (2) identifiable private information."

We turn to authorities such as the **Belmont and Menlo Reports** to guide ethical thinking.

Frequently consult with colleagues to check our reasoning and conclusions.

Questions we regularly consider include:

- **What populations of users are affected?**
- **Is informed consent feasible?**
- **Have we considered all anticipatable risks?**
- **Do humans incur no more than minimal risk?**
- **Can we take steps to further reduce risks?**
- **Do benefits accrue to the population that is subjected to the risk?**

From (Raw) Data points to Understanding Censorship?

Side channels

TCP/IP Layer
→ Spooky (2014)
→ Augur (2017)

DNS Layer
→ Satellite (2017)

Application Layer
→ Quack (2018)
→ HyperQuack (2020)

 Challenges 

➔ Disruption detection is not necessary censorship detection

➔ Ambiguity in location and granularity of filtering

➔ The techniques are each specialized to detect one type of censorship, and have only been used for a single snapshot in time

Building Censored Planet Observatory

NEED: A platform for continuously monitoring global Internet censorship

We build Censored Planet:

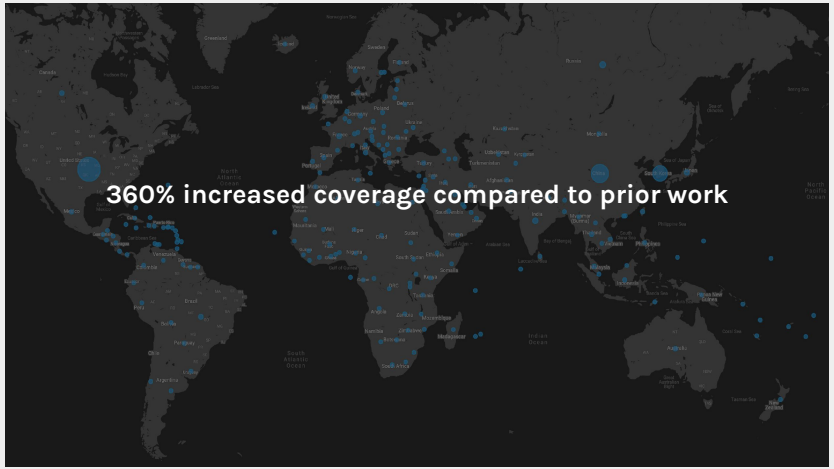
- ➔ **Orchestrate running remote measurement techniques**
- ➔ **Use data science to distill understanding**
- ➔ **Disseminate and facilitate data use**

* **Censored Planet: An Internet-wide, Longitudinal Censorship Observatory**
R. Raman, P. Shenoy, K. Kohls, R. Ensafi
ACM CCS 2020

Orchestrate Running Side Channels

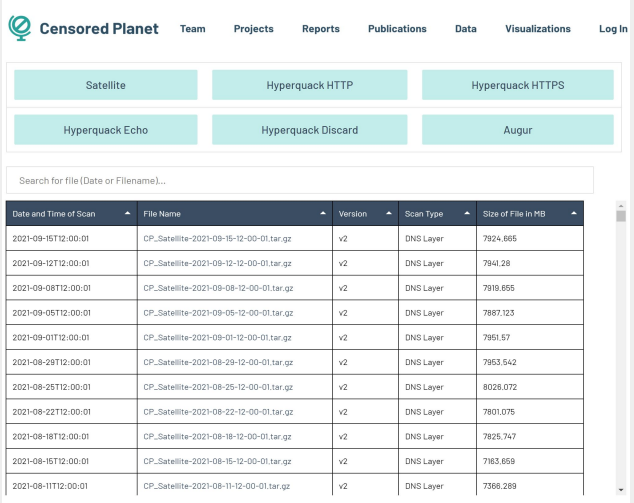
Censored Planet

From August 2018, **been running these side channels in parallel continuously testing reachability to 2000 sensitive domains from 95,000 vantage points!**



94 billion data points

Largest public censorship dataset

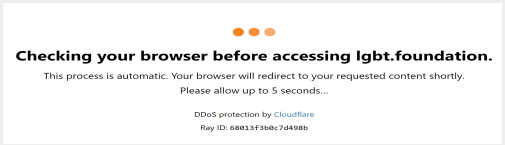


Challenges with Analyzing Censorship

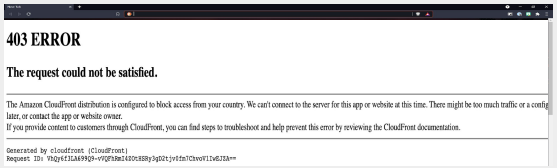
Unexpected anomalies

1. CDN behavior

2. Bot detection

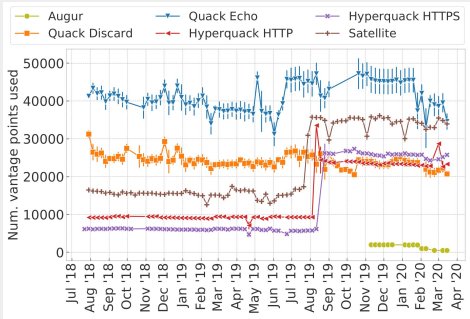


3. Geoblocking

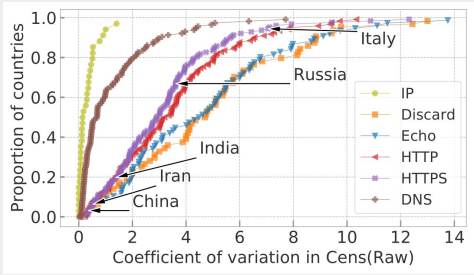


Temporal & Spatial Variance

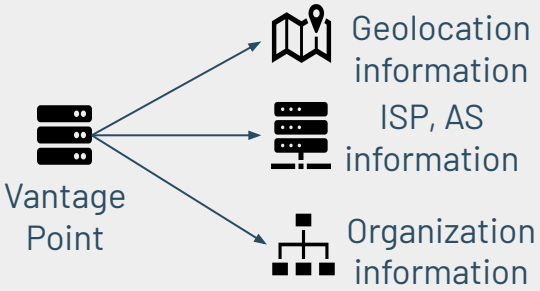
1. Vantage Point Changes



2. Organizational Policies



Insufficient Metadata



Variance in Errors

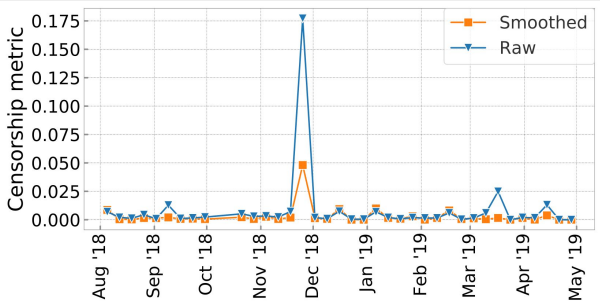
Error Types
Resets
Timeout
DNS errors
TLS/HTTP errors

Analyzing Censorship

Building universal data schema
— that covers all techniques

Obtain a representative metric of censorship
— not every vantagepoint is equally weighted within a country

Dealing with outlier vantage points
— apply an **optimization model** (Nelder-Mead) to obtain a weight for each Autonomous System that smooths the metric.



Trend Analysis - Mann-Kendall test

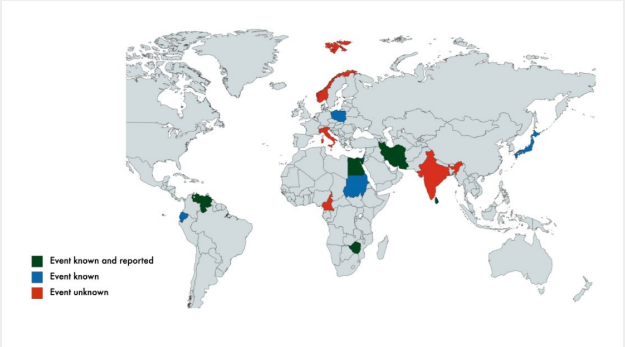
— Increasing levels of DNS censorship >100 countries.

— HTTPS censorship showing increasing trend.

— 11 categories of domains increasingly blocked
e.g., News Media, Provocative Attire.

Anomaly Detection - Bitmap-based detection

— Identified 15 key censorship events

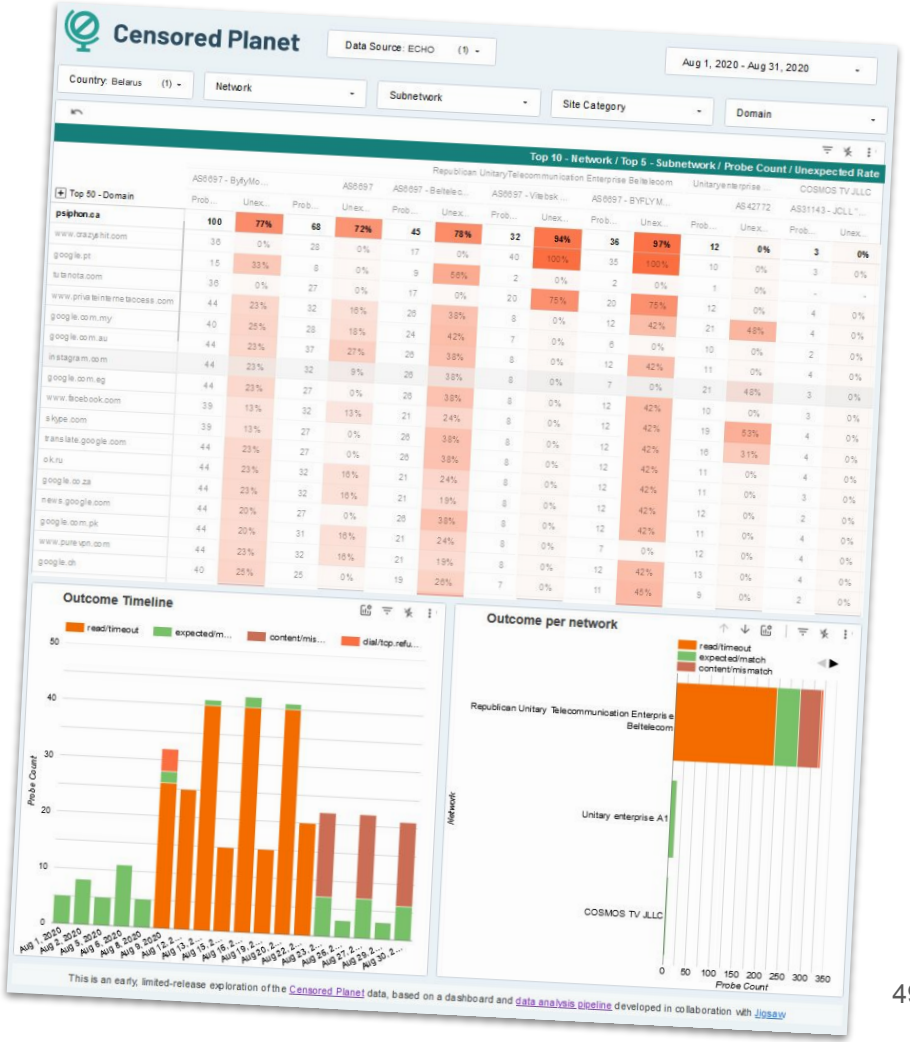


Censored Plant Dashboard

Developed in collaboration with Google's Jigsaw

To facilitate data use and enable easy visualizations, we built our dashboard that automatically gets updates after each scans.

We provide free access to our data users.



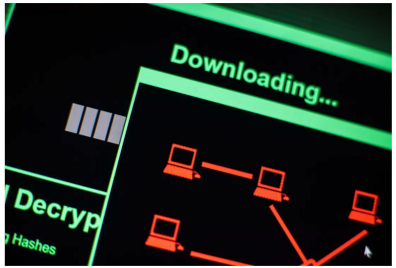
Censored Planet Rapid Response

Censored Planet team has exposed **significant new government censorship tactics**, and our results have been highlighted in more than 100 popular press articles.

Google, Apple and Mozilla to block internet surveillance in Kazakhstan

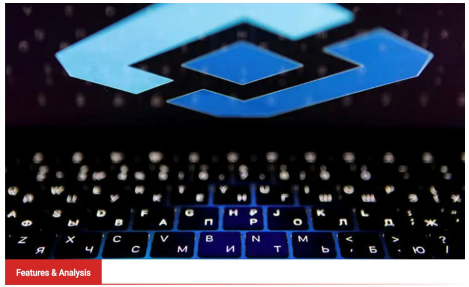
It's a response to the government's attempt to intercept users' browser data.

Oscar Gonzalez
Aug. 21, 2019 7:02 a.m. PT



The makers of the most popular browsers are taking a stand against the Kazakh government.

Picture Alliance/Getty Images



Features & Analysis

Laws, cheap web filters arm Russia to block news, says Censored Planet

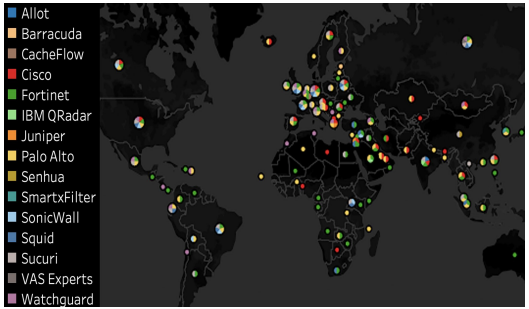
By Madeline Earp/CPJ Consultant Technology Editor on November 7, 2019 11:36 AM EST

When Daniil Kislov tried to view the website of *Fergana* from his computer in Moscow on November 1, his browser showed

STORIES

Roskomnadzor successfully slows down Twitter. American researchers explained how he did it. They even found a small loophole for users - it's a pity that it's unlikely to help them

01:36, April 8, 2021
Source: Meduza



Real-time monitor tracks the growing use of network filters for censorship

February 21, 2020

The team says their framework can scalably and semi-automatically monitor the use of filtering technologies for censorship at global scale.

Censored Planet

Research papers

IMC '21
Throttling Twitter: an emerging censorship technique in Russia

FC '21
Lost in Transmission: Investigating Filtering of COVID-19 Websites

CCS '20
Censored planet: an internet-wide, longitudinal censorship observatory

IMC '20
Investigating large scale HTTPS interception in Kazakhstan

NDSS '20
Decentralized Control: A Case Study of Russia

NDSS '20
Measuring the deployment of network censorship filters at global scale

USENIX '18
Quack: Scalable Remote Measurement of {Application-Layer} Censorship

S&P '17
Augur: Internet-wide detection of connectivity disruptions

IEEE Security & Privacy '18
Toward continual measurement of global network-level censorship

USENIX '17
Global measurement of {DNS} manipulation

IMC '17
A look at router geolocation in public and commercial databases

NS ETHICS '15
Ethical Concerns for Censorship Measurement

PETS '15
Analyzing the Great Firewall of China Over Space and Time.

PAM '14
Detecting intentional packet drops on the Internet via TCP/IP side channels

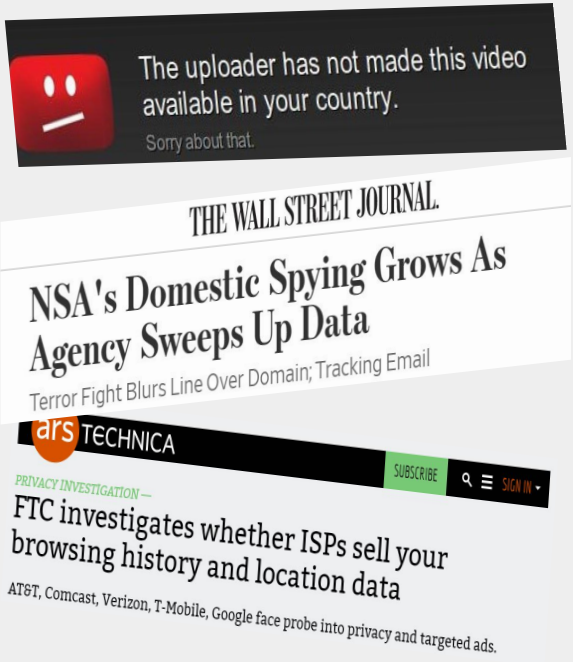
Safeguarding the consumer VPN ecosystem

"All of them claim to be the best": Multi-perspective study of VPN users and VPN providers
R. Ramesh, A. Vyas, R. Ensafi
Under submission

OpenVPN is Open to VPN Fingerprinting
D. Xue, R. Ramesh, M. Kallitsis, J. Halderman, J. Crandall, R. Ensafi
USENIX Security, August 2022

VPNalyzer: Systematic Investigation of the VPN Ecosystem
R. Ramesh, L. Evdokimov, D. Xue,R. Ensafi
NDSS, Apr 2022

VPNs are on the Rise



"From 2010 to year-end 2019, the use of VPNs has increased by **approximately four times"**
American cybersecurity company PC Matic

"VPN usage increased 3% week over week and hit a new peak at 81% higher than a typical pre-COVID day"
Verizon Network Report, May, 2020

Reasons:
Protection from surveillance, censorship circumvention, accessing work/school/university resources, circumventing geo-blocking, entertainment, etc

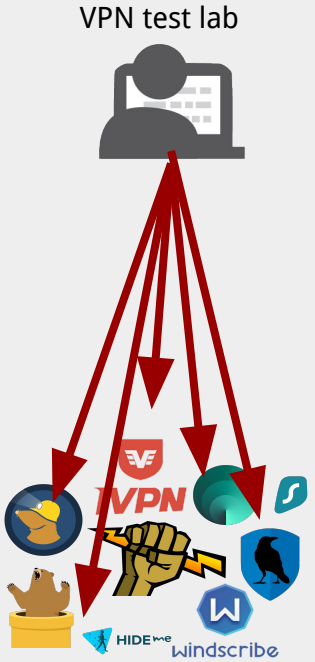
This multibillion-dollar industry includes many snakeoil products, hyperbolic claims, is laxly regulated, and remains severely understudied.

Challenges to Investigating VPNs

Previous reports are lab-based:

- Used inconsistent heuristics that prevent monitoring of issues over time (unsystematic investigation)
- Limited in the scale and types of VPN products (covering only a small slice of the market)
- Involved a large amount of manual effort

KEY CHALLENGE:
Rigor, Scale, Automation



We built VPNalyzer

to address these challenges

Building VPNalyzer to Address Key Challenges

Repeated VPN evaluations over time **should not require** starting from scratch

Testing and validating VPN providers' fixes for issues reported as disclosures requires an easily updatable test suite

VPNalyzer must adopt a modular, extensible test suite implementation

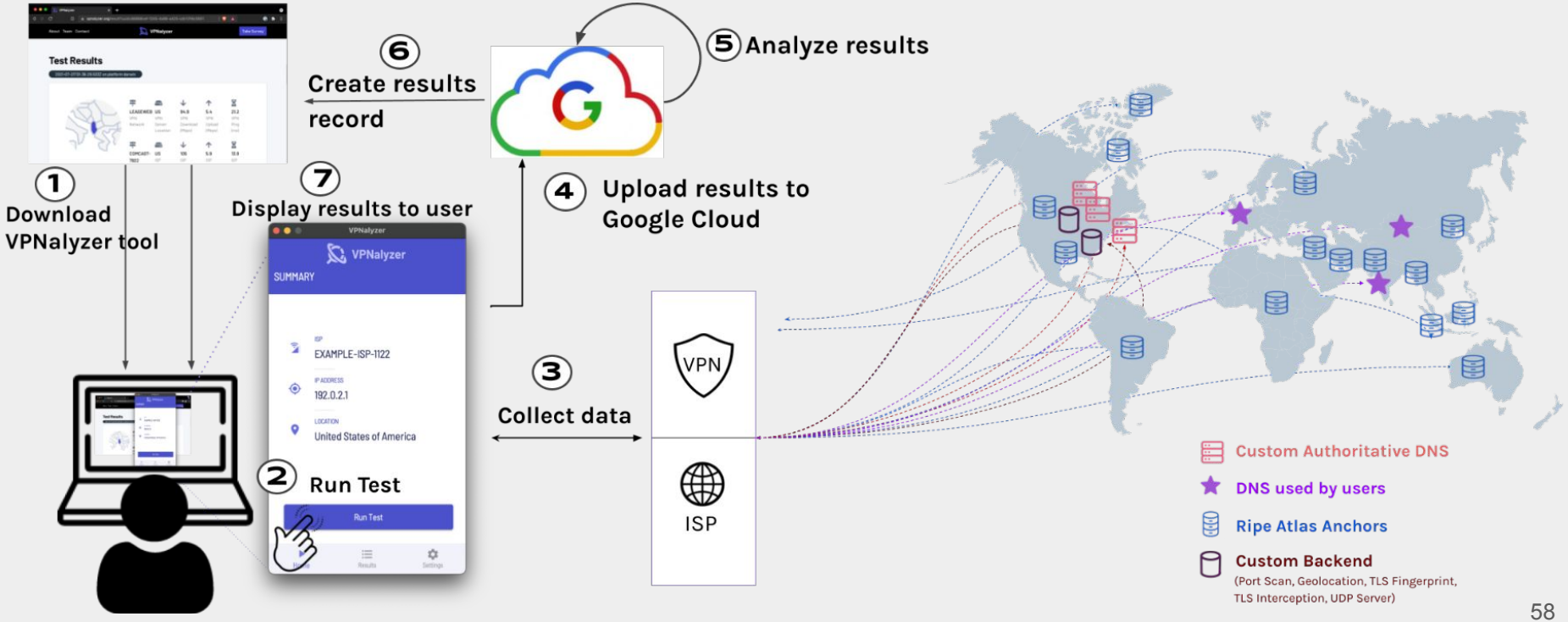
VPN ecosystem has increasing:

- number of VPN providers
- number of users w/ varied threat models
- use cases

VPNalyzer must facilitate large-scale crowd-sourced measurements

VPNalyzer System Design

User-friendly tool with a one-click install process for Windows, MacOS, and Linux



What do we test with VPNalyzer?

VPNalyzer has a modular, extensible test suite covering aspects of performance, security, and privacy

Aspects of Service

Bandwidth and latency

Geolocation

RPKI validation

Misconfiguration and Leakages

DNS leaks

IPv6 leaks

Data leaks during tunnel failure

Security and Privacy Essentials

Lack of support for DoH

TLS Interception

Port scanning

Router interface reachability

Presence of DNS proxy

QNAME minimization

Testing VPNalyzer

We tested VPNalyzer with **80 popular VPNs** and uncovered dozens of previously unreported problems

We tested random servers in each VPN provider, on Windows and MacOS for VPN default and secure mode:

- **58 paid** VPN providers
- **18 free** VPN providers
- **4 self-hosted** VPN solutions
  (Algo, OpenVPN Access Server on AWS, Outline, Streisand)

VPNalyzer Findings: Misconfiguration and Leakages

VPNalyzer found evidence of many traffic leaks, which seriously risk exposing sensitive user data.

IPV6 traffic

Only 14% support IPv6

Five VPNs leak IPv6 traffic to the ISP by default

UMich VPN is among them

During tunnel failure

In default configuration, **33% of providers leak traffic** to the user's ISP

Even in their most secure setting, 10 providers leak traffic to the user's ISP

Insecure default configuration

Misleading default configuration caused (non-browser) traffic to be exposed to the ISP

Astrill VPN and Psiphon tunneled only browser traffic by default

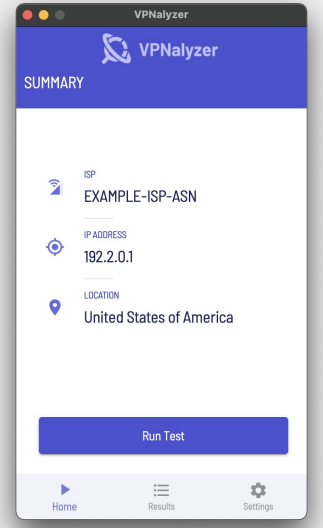
VPNalyzer team filed 26 disclosure to these VPNs due to security and privacy risk exposing sensitive user data through traffic leaks

What's Next: Deployment and Crowdsourcing

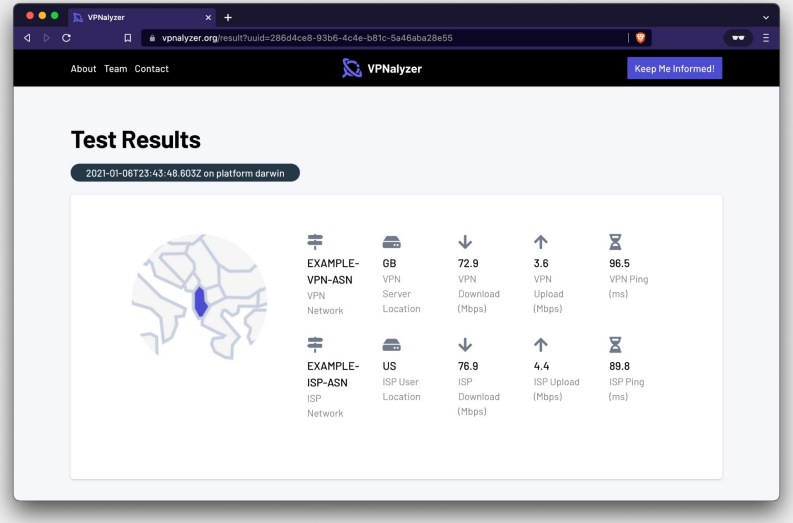
VPNalyzer Tool beta-launched at NDSS 2022 🎉

Crowdsourced study:

- Help scale coverage to many hundreds of providers
- Study region-specific VPNs that are often overlooked

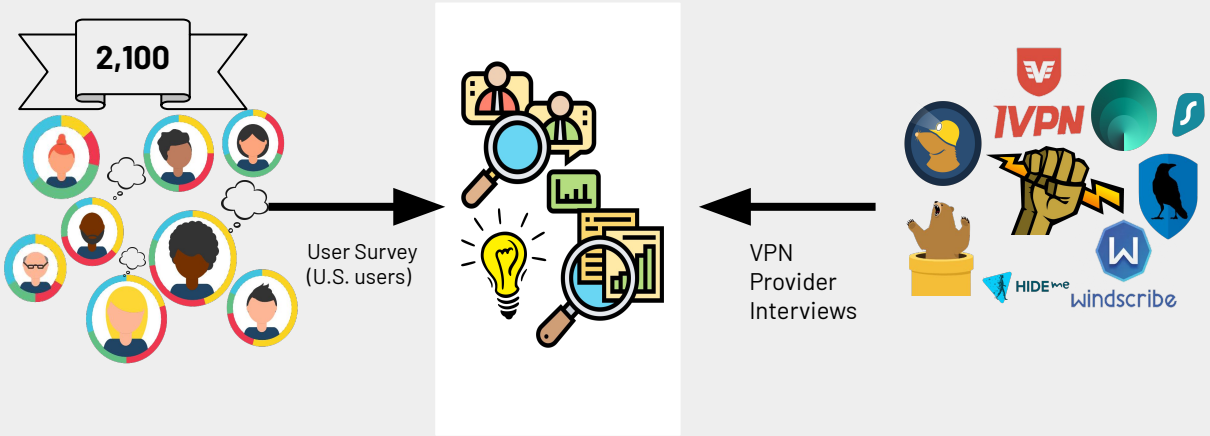


For the future, crowdsourcing will provide continuous data from users to spot new problems, monitor fixes for known issues, and keep findings up to date



Measuring the Efficacy of Currently Deployed Tools

Understanding the user needs and considerations, and VPN providers to bridge gaps and highlight (mis)aligned incentives



"All of them claim to be the best": Multi-perspective study of VPN users and VPN providers R. Ramesh, A. Vyas, R. Ensafi, Under Submission

Multi-perspective study of VPN users and VPN providers

CR Consumer Reports

With support from Consumer Reports, our survey received 2,100 responses from > 40 countries

User study highlight:

86.7% of users feel somewhat/very safe using a VPN

40% of users have a flawed mental model of the security their VPN provides (no significant difference between users of different expertise)

57% of users are highly reliant on VPN recommendation sites (of whom 94% rate them trustworthy)

VPN provider highlight:

VPN providers reveal recommendation sites are largely **not objective** and instead are **motivated by profit**

"You honestly cannot find even one ranking site that is honest, if you just tell people that…so that people know"

Multi-perspective study of VPN users and VPN providers

Consumer Reports

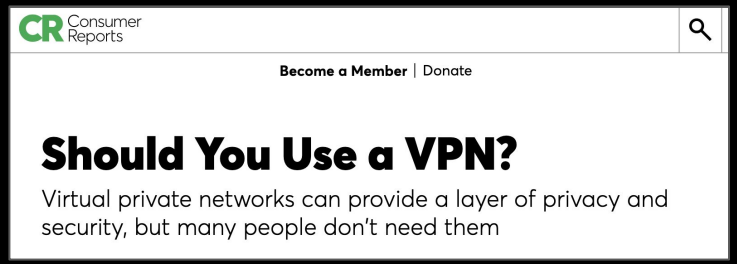
With support from Consumer Reports, our survey received 2,100 responses from > 40 countries

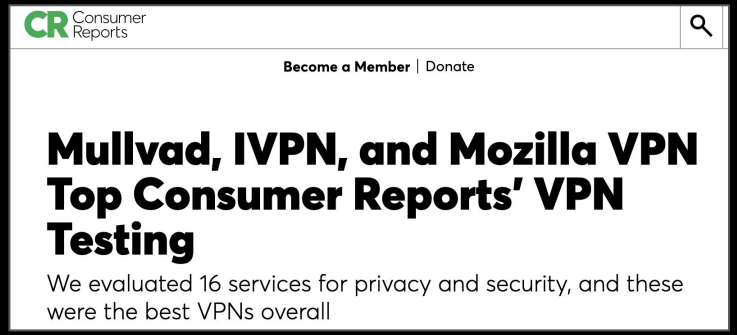
Big lesson:

- **Prioritizing user education**
- **Oversight on advertisements and marketing surrounding VPNs**
- **Regulations to curb misleading marketing that leads to flawed mental models**

VPNalyzer Impact

Consumer Reports used our **VPNalyzer tool** for their own investigation to help recommend VPNs to their millions of subscribers

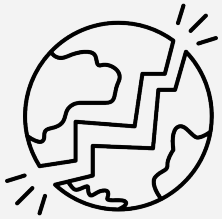




Other work:

Investigating the Geo-inequity of users' online experiences

splintering.net

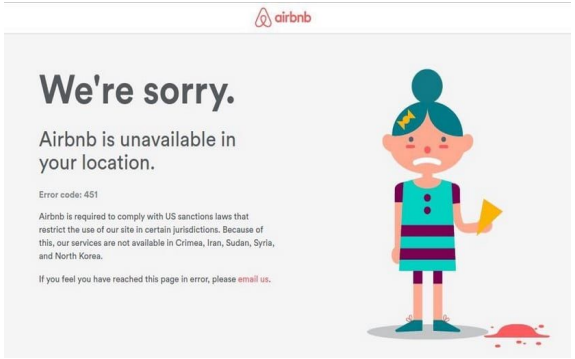


The Impact of Geoblocking and the U.S. Embargo on Internet Freedom in Cuba
A Ablove, R Sundra Ramen, R Ramesh, S. Chandrashekaran, Y. UeharaD. Madory, R. Ensafi
Under Submission

A large-scale investigation into geo-differences in mobile apps.
R. Kumar, A. Virkud, R. Sundara Raman,A. Prakash,R. Ensafi.
In USENIX Security, 2022.

403 Forbidden: A Global View of CDN Geoblocking
A. McDonald, M. Bernhard, B. VanderSloot, W. Scott, A. Halderman, R. Ensafi
ACM Internet Measurement Conference (IMC), November 2018

Server-side geo-discrimination is on the rise→ Balkanization of Internet



Los Angeles Times

Unfortunately, our website is currently unavailable in most European countries. We are engaged on the issue and committed to looking at options that support our full range of digital offerings to the EU market. We continue to identify technical compliance solutions that will provide all readers with our award-winning journalism.

Measuring geo-blocking

Why do sites Geoblock?

Sites may attempt to minimize fraud or **combat abuse.**

Iran, Syria, Sudan, North Korea and Cuba are under **U.S. sanctions**, some companies block access to comply.

Increasingly CDNs make it easy to block sites by a click by offering a easy accable country-level blocking tool in their client's portal.

Impact: Subsequent to our study, **CloudFlare disabled geoblocking** for all but Enterprise customers.

CLOUDFLARE®

Other works:

A first large-scale investigation into geo-differences in mobile apps. [USENIX Security 2022]

The Impact of Geoblocking and the U.S. Embargo on Internet Freedom in Cuba

The New York Times

Study: Russia's Web-Censoring Tool Sets Pace for Imitators

By The Associated Press

Nov. 6, 2019

WASHINGTON — Russia is succeeding in imposing a highly effective internet censorship regime across thousands of disparate, privately owned providers in an effort also aimed at making government snooping pervasive, according to a study released Wednesday.

FINANCIAL TIMES

US-China relations + Add to myFT

US blocks Hong Kong users from some government websites

Sites hosting economic data have been inaccessible to users in the Asian financial centre for months

ars TECHNICA SUBSCRIBE

THE REVOLUTION WILL NOT BE TWEETED —

Russia's Twitter throttling may give censors never-before-seen capabilities

BBC NEWS

Home Video World UK Business Tech Science

Technology

MIT Technology Review Subscribe

MS TECH

Q&A

Why you should be more concerned about internet shutdowns

WIRED SUBSCRIBE

CHRIS STOKEL-WALKER SECURITY APR 1, 2022 7:00 AM

Russia Inches Toward Its Splinternet Dream

For years, the country has been trying to create its own sovereign internet—a goal given new impetus by the backlash to its invasion of Ukraine.

Russia Is Censoring the Internet, With Coercion and Black Boxes


By Adam Satariano and Paul Mozur

zilla move to s
ooping'

The Economist

nternational

Oct 16th 2021 edition ›

ockheads

Governments are finding new ways to squash free expression online

Real-time monitor tracks the growing use network filters for censorship

MICHIGAN RADIO npr 91.7 Ann Arbor/Detroit 104.1 Grand Rapids 91.3 Port Huron 89.7 Lansing 91.1 Flint

Donate

News

Research team investigating Internet censorship with tracking system

Michigan Radio | By Lauren Janes

Published February 6, 2019 at 4:38 PM EST

Forbes

CYBERSECURITY

Apple, Google And Mozilla Block Kazakh Government Surveillance

Emma Woollacott Senior Contributor

Follow

'Extremely aggressive' internet censorship spreads in the world's democracies

Roskomnadzor successfully slows down Twitter. American researchers explained how he did it. They even found a small loophole for users - it's a pity that it's unlikely to help them

01:36, April 8, 2021


SUMMIT FOR
DEMOCRACY


U.S.-GERMAN
FUTURES FORUM
DEUTSCH-AMERIKANISCHES
ZUKUNFTSFORUM
The Future of Democracy
in a Digital World


Auswärtiges Amt
BertelsmannStiftung
U.S.-GERMAN
FUTURES FORUM
DEUTSCH-AMERIKANISCHES
ZUKUNFTSFORUM
The Future of Democracy
in a Digital World
November 2-3, 2022
Münster, Germany

Protecting Users from Adversarial Networks

Roya Ensafi
University of Michigan