CSE227 – Graduate Computer Security

More DDoS, Network Censorship

UC San Diego

Housekeeping

General course things to know

- Midpoint check-in document is due **5/8 at 11:59pm PT**
  - Introduction (frame the problem)
  - Related work section (should include ~5 – 10 relevant papers)
  - Research plan, current status, what's left to do
  - **Due on Gradescope!**
- Midpoint check-in meetings will happen week 7!
  - I sent out Calendly's… please sign up! Take 5 mins with your group **right now**

Today's lecture

Learning Objectives

- Discuss the "Takedown" paper
- Discuss network censorship (10K foot)
- Discuss the "Wallbleed" paper

Where we left off…

- DDoS (Distributed Denial of Service) is an attack that threatens the *availability* of a system…
  - Mostly, we spoke last week about *flooding* DDoS, wherein a litany of devices are used to knock out the resources of an external entity
- Today — **what happens when you take DDoS offline?**

Assessing the Aftermath: the Effects of a Global Takedown against DDoS-for-hire Services

DDoS-for-hire Fundamentals

- What is a booter service?
- What do people use booter services for?
- What kinds of attacks are typically attributed to booters?

Booter Takedowns

PRESS RELEASE

U.S. authorities conduct cyber operations as part of global crackdown on DDoS-for-hire services

Thursday, April 16, 2026

Share

For Immediate Release

U.S. Attorney's Office, District of Alaska

ANCHORAGE, Alaska – The U.S. Justice Department today announced court-authorized actions taken to disrupt some of the world's leading Distributed Denial of Service (DDoS) Internet of Things (IoT) botnet services.

U.S. authorities continue to focus resources on charging DDoS botnet administrators and seizing infrastructure, like websites, that allow paying users to launch powerful DDoS attacks. These attacks flood targeted computers and servers with information to prevent them from being able to access the internet. In recent years, DDoS, aka "booter," services have continued to proliferate as they offer a low barrier to entry for users looking to engage in cybercriminal activity.

DDoS services, such as those named in this action, allegedly attacked a wide array of victims in the United States and abroad, including schools, government agencies, gaming platforms, critical infrastructure, including Department of War resources, and millions of people. In addition to affecting targeted victims, these attacks can significantly degrade internet services and completely disrupt internet connections.

- What strategies does law enforcement use to conduct a booter takedown?

Booter Takedowns

PRESS RELEASE

U.S. authorities conduct cyber operations as part of global crackdown on DDoS-for-hire services

Thursday, April 16, 2026

Share

For Immediate Release

U.S. Attorney's Office, District of Alaska

ANCHORAGE, Alaska – The U.S. Justice Department today announced court-authorized actions taken to disrupt some of the world's leading Distributed Denial of Service (DDoS) Internet of Things (IoT) botnet services.

U.S. authorities continue to focus resources on charging DDoS botnet administrators and seizing infrastructure, like websites, that allow paying users to launch powerful DDoS attacks. These attacks flood targeted computers and servers with information to prevent them from being able to access the internet. In recent years, DDoS, aka "booter," services have continued to proliferate as they offer a low barrier to entry for users looking to engage in cybercriminal activity.

DDoS services, such as those named in this action, allegedly attacked a wide array of victims in the United States and abroad, including schools, government agencies, gaming platforms, critical infrastructure, including Department of War resources, and millions of people. In addition to affecting targeted victims, these attacks can significantly degrade internet services and completely disrupt internet connections.

- What strategies does law enforcement use to conduct a booter takedown?
  - Seize domains, arrest and charged people running the websites, infiltration of dark web pages
  - *Advertising* for deterrance

This paper

- **What happened to the DDoS-for-hire ecosystem post intervention?**
- How they did it…
  - How did the authors collect ground truth traffic on booter domains?
  - What is a honeypot? How did the authors use honeypot data in their analysis?
  - What social platforms helped the authors in their analysis?

Table 1: The quantitative data sources used and their origins.

Datasets	Statistics	Origins
Ground-truth traffic ◇	20.7M raw events	Our collection
Similarweb analytics ⋆	94 booter domains	Our collection
HOPSCOTCH †	4.6M records	Thomas et al. [38]
AMPPOT †	9.8M records	Krämer et al. [39]
NETSCOUT †	32.9M records	NETSCOUT [40]
Self-reported statistics †	207 booters	Our collection
Underground forums ⋆	1 704 posts	Pastrana et al. [41]
Chat channels ⋆	34 438 messages	Our collection

Data timespans covering both waves: ◇ [14 December 2022 – 31 July 2023]; ⋆ [1 October 2022 – 30 September 2023]; † [1 July 2021 – 30 June 2023]

Resurrections

- How quickly did booter services “resurrect” themselves?
  - Hours to days; **high resurrection rate!**
- First wave had ~50% resurrection, second had 100% resurrection!
  - Booters were highly resilient

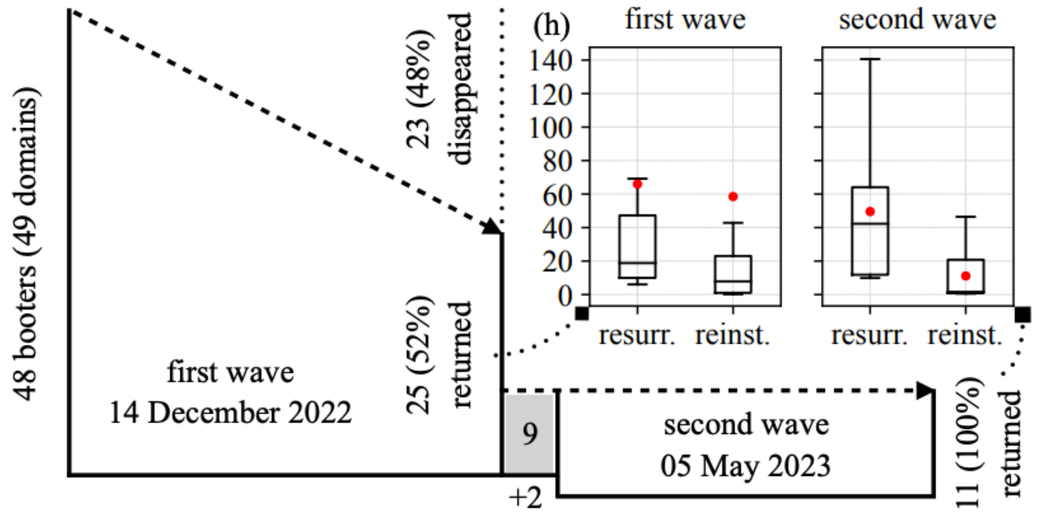
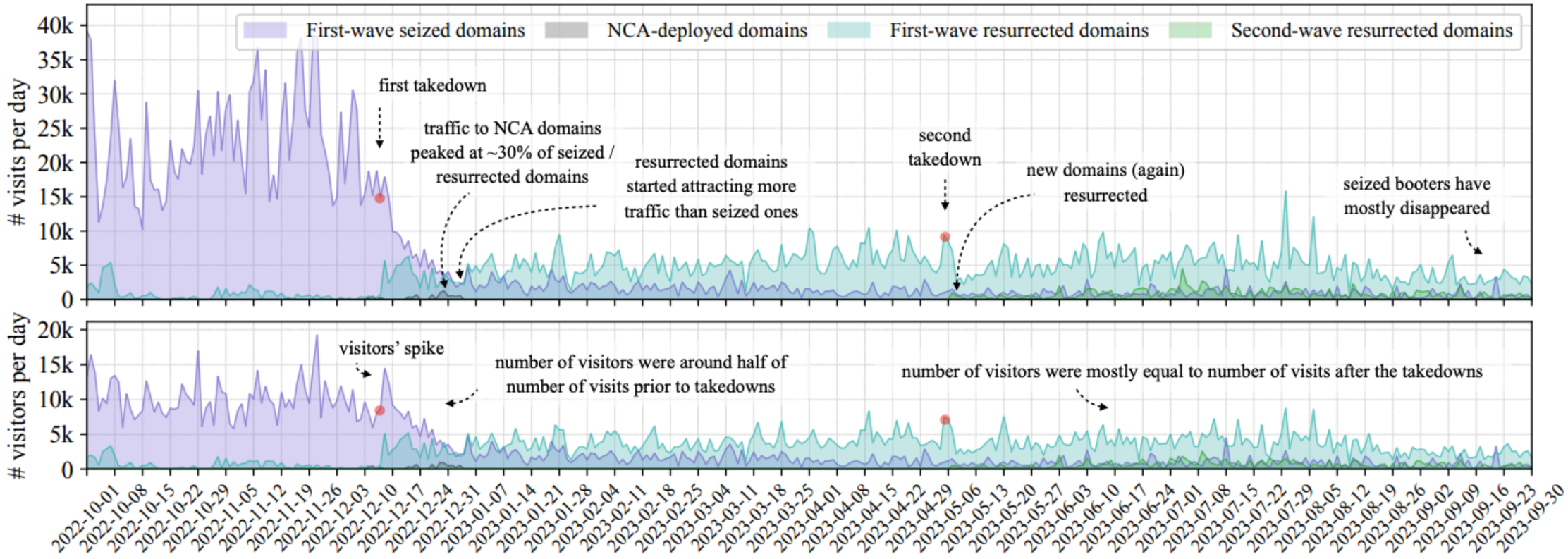


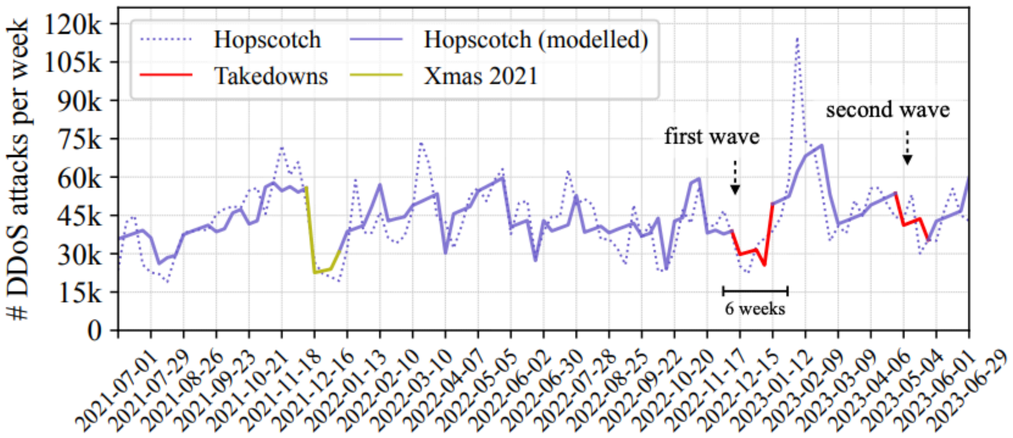
Figure 1: Overview of booter resurrections and reinstallations after two waves of takedown (hours). Red dots indicate means.

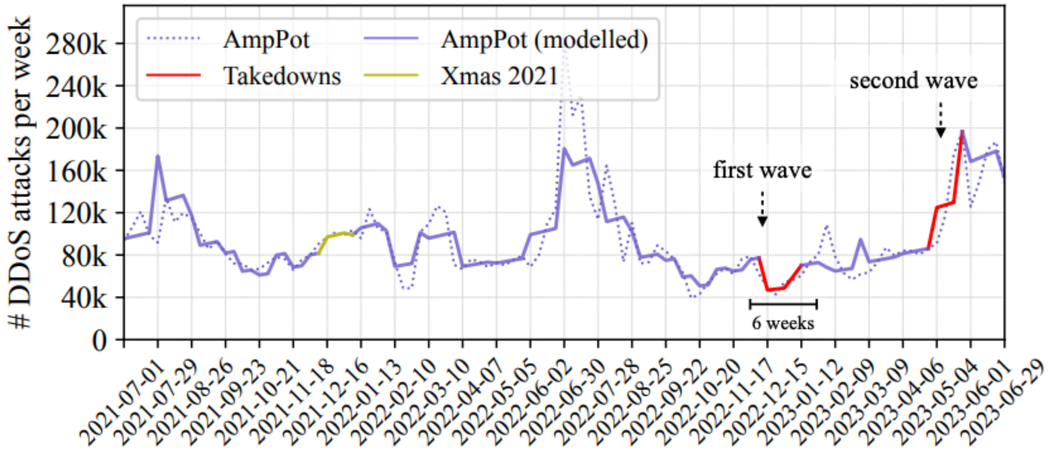
Longitudinal effects on supply-side traffic



Traffic *significantly* decreased due to the intervention (90% reduction)

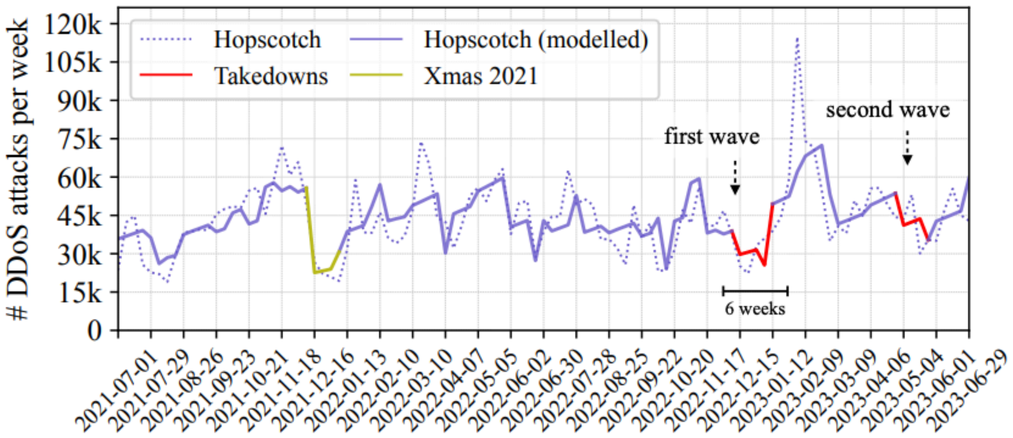
Longitudinal effects on demand

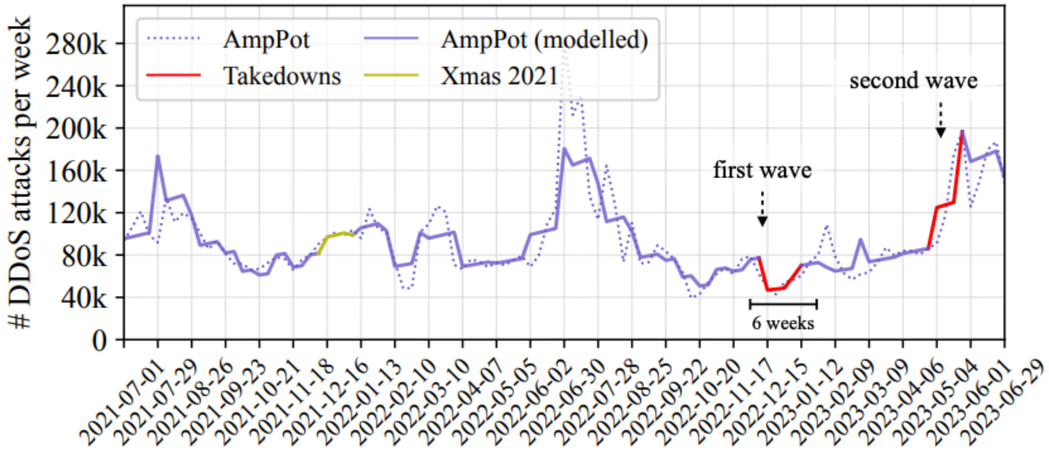




How did these interventions impact the demand for DDoS attacks?

Longitudinal effects on demand





How did these interventions impact the demand for DDoS attacks?

Immediate reduction; but regression back to mean in ~6 weeks.

Meta-thoughts

- Takedowns of supply have a *short-lived* effect in this ecosystem. Why? What does this tell us about these types of interventions?
  - Where might these interventions be useful? Where might they not be?
- What *surprised* you about this paper? What didn't surprise you at all?
- What did this paper make you think about *trust*?

Break Time + Attendance

https://tinyurl.com/cse227-attend

Codeword:
CensorYou!

Network Censorship Preliminaries

What is censorship?

What is censorship?

Censorship: The suppression of words, images, ideas that are “offensive,” typically an arm for political or personal control or coercion

What is Internet censorship?

What is Internet censorship?

Internet censorship: Censorship on the Internet – and typically enacted via technical, network-level means

How Internet Censors Work

Major mechanisms for running Internet Censorship

- What is an Internet shutdown?

How Internet Censors Work

Major mechanisms for running Internet Censorship

- What is an Internet shutdown?
  - Removing Internet service altogether – much easier in some countries than others

How Internet Censors Work

Major mechanisms for running Internet Censorship

- What is an Internet shutdown?
  - Removing Internet service altogether – much easier in some countries than others
- What is throttling?

How Internet Censors Work

Major mechanisms for running Internet Censorship

- What is an Internet shutdown?
  - Removing Internet service altogether – much easier in some countries than others
- What is throttling?
  - Making certain services slower in country boundaries

How Internet Censors Work

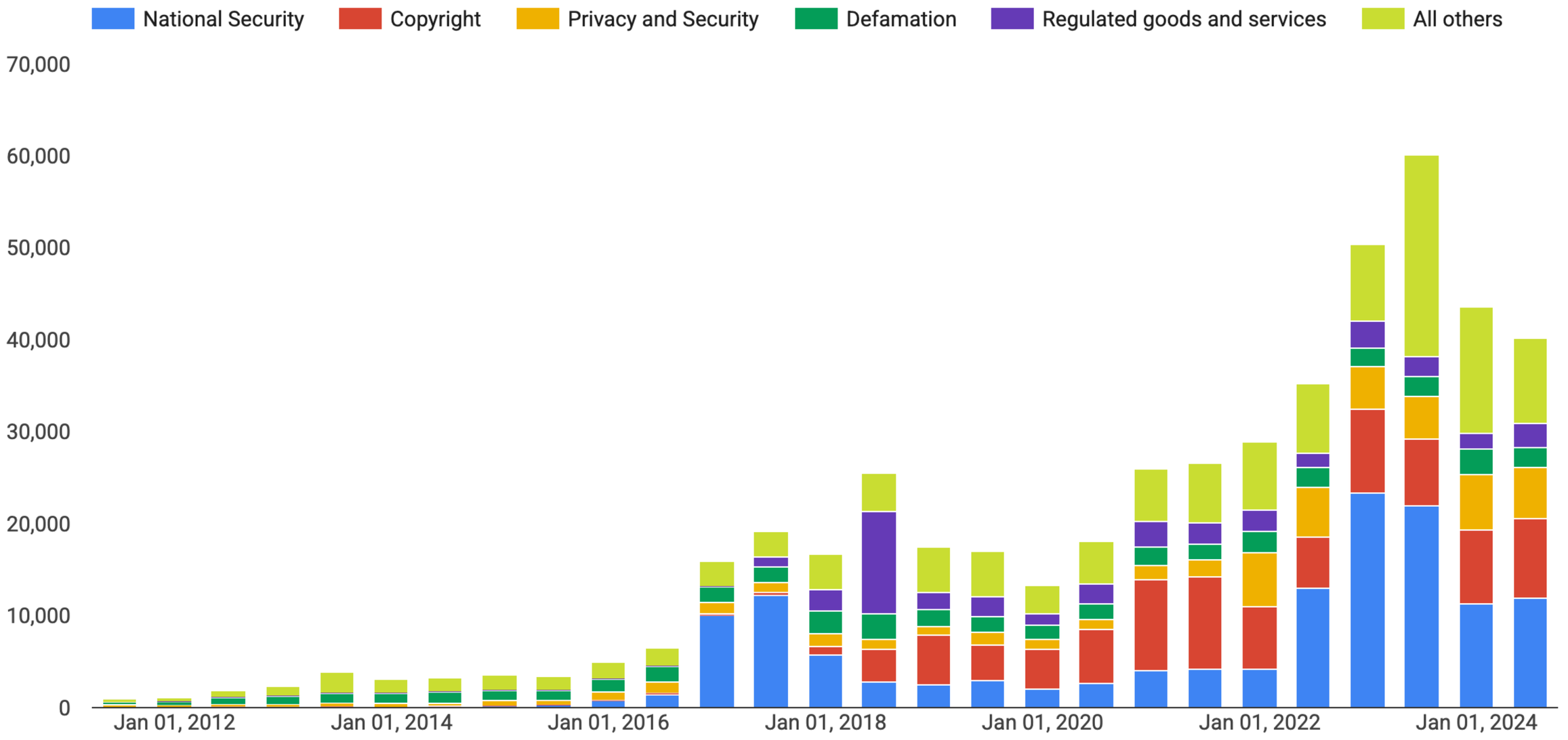
Major mechanisms for running Internet Censorship

- What is an Internet shutdown?
  - Removing Internet service altogether – much easier in some countries than others
- What is throttling?
  - Making certain services slower in country boundaries
- What are content takedowns?

How Internet Censors Work

Major mechanisms for running Internet Censorship

- What is an Internet shutdown?
  - Removing Internet service altogether – much easier in some countries than others
- What is throttling?
  - Making certain services slower in country boundaries
- What are content takedowns?
  - Removal of “offensive” content from online services


National Security
Copyright
Privacy and Security
Defamation
Regulated goods and services
All others
70,000
60,000
50,000
40,000
30,000
20,000
10,000
0
Jan 01, 2012
Jan 01, 2014
Jan 01, 2016
Jan 01, 2018
Jan 01, 2020
Jan 01, 2022
Jan 01, 2024

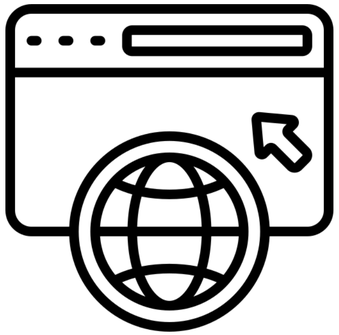
How Internet Censors Work

Major mechanisms for running Internet Censorship

- Primary form of Internet censorship: network-level blocking
- Three main ways that network-level blocking happens in practice
  - What is DNS manipulation?

Censorship during an Internet connection

Modes of website blocking

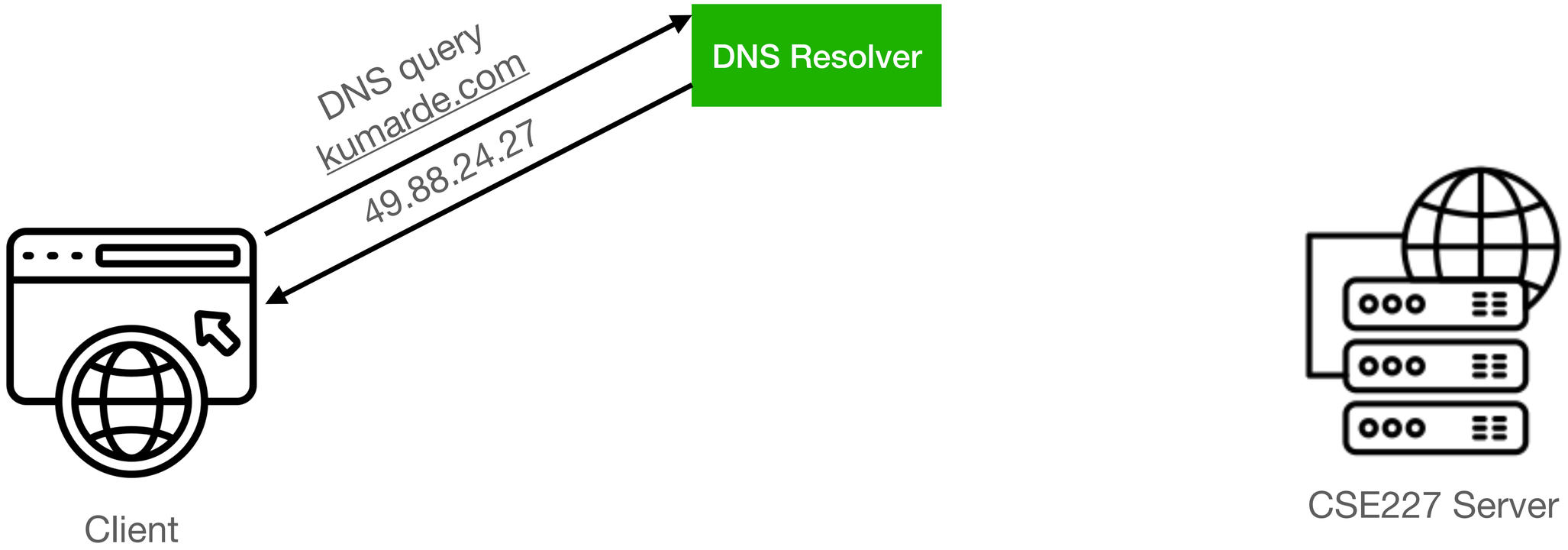


Client

CSE227 Server

Censorship during an Internet connection

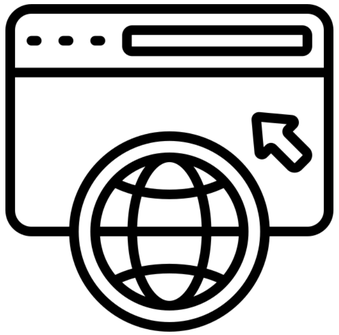
DNS Manipulation



Censorship during an Internet connection

DNS Manipulation

DNS Resolver



Client

CSE227 Server

Censorship during an Internet connection

DNS Manipulation

Censorship during an Internet connection

DNS Manipulation

How easy do we think this is to implement?

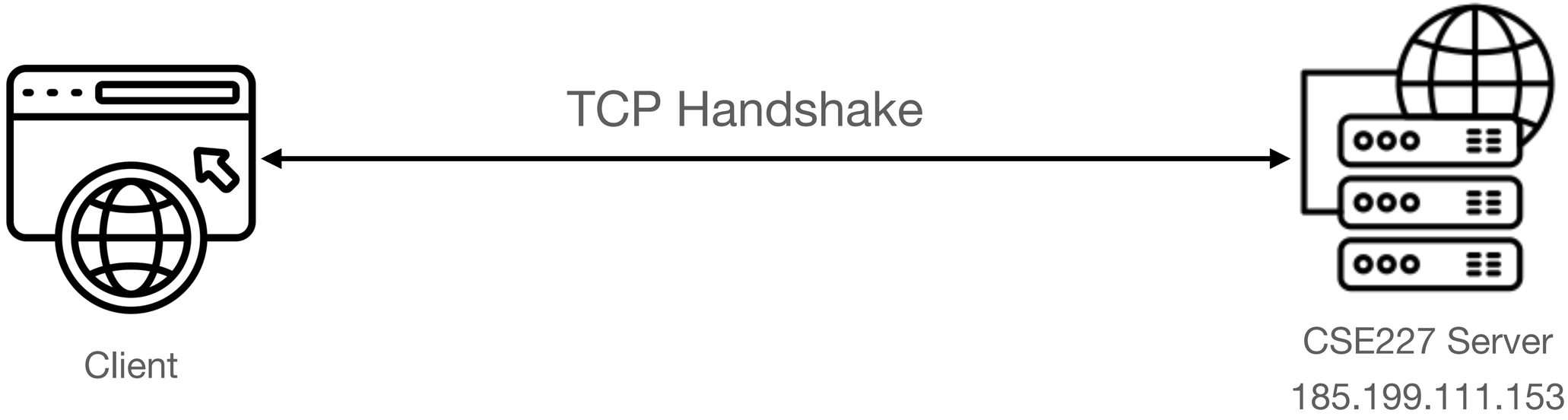
How Internet Censors Work

Major mechanisms for running Internet Censorship

- Primary form of Internet censorship: network-level blocking
- Three main ways that network-level blocking happens in practice
  - What is DNS manipulation?
  - What is IP blocking?

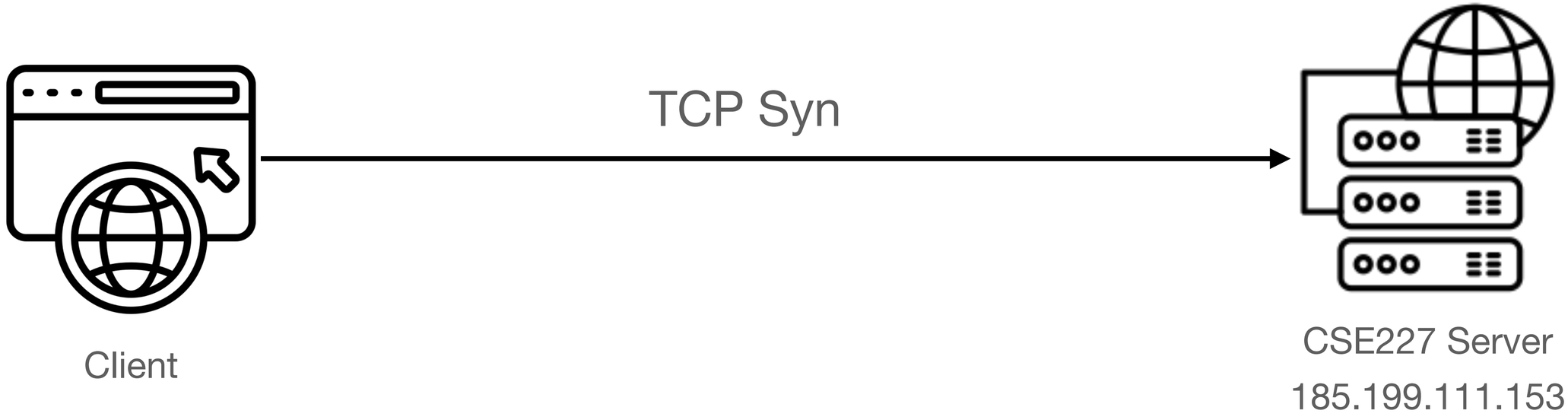
Censorship during an Internet connection

IP Blocking



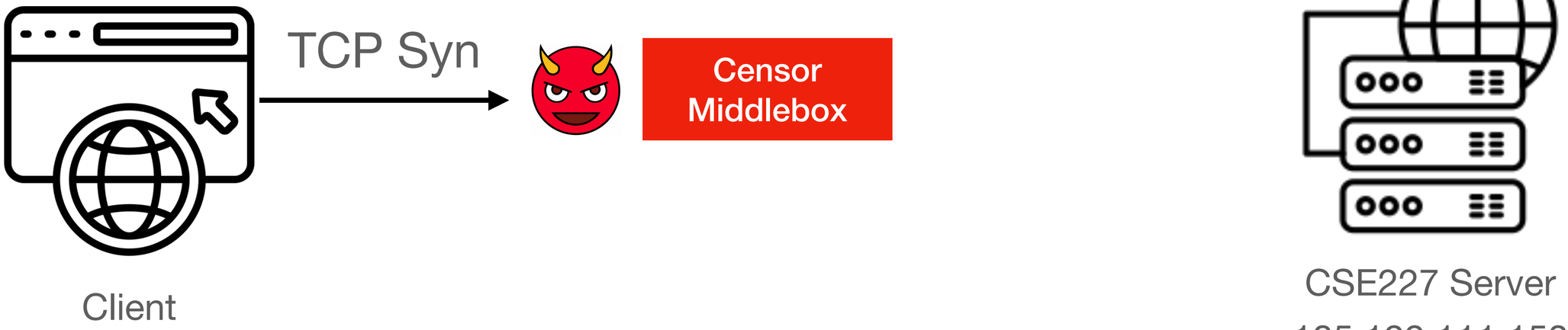
Censorship during an Internet connection

IP Blocking



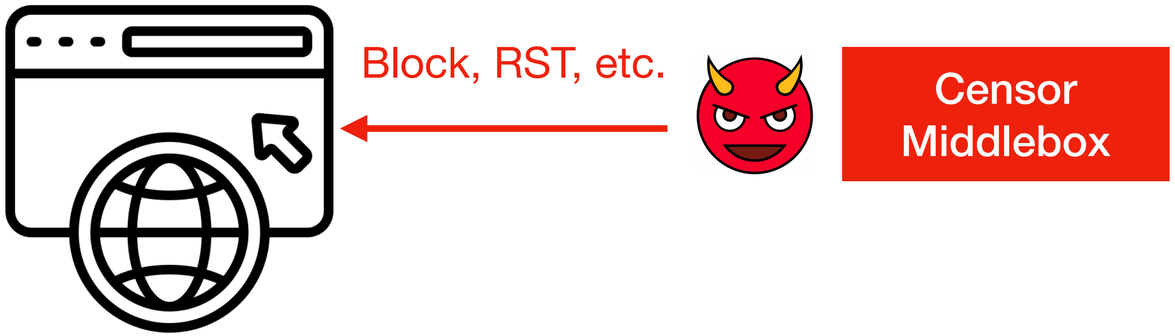
Censorship during an Internet connection

IP Blocking



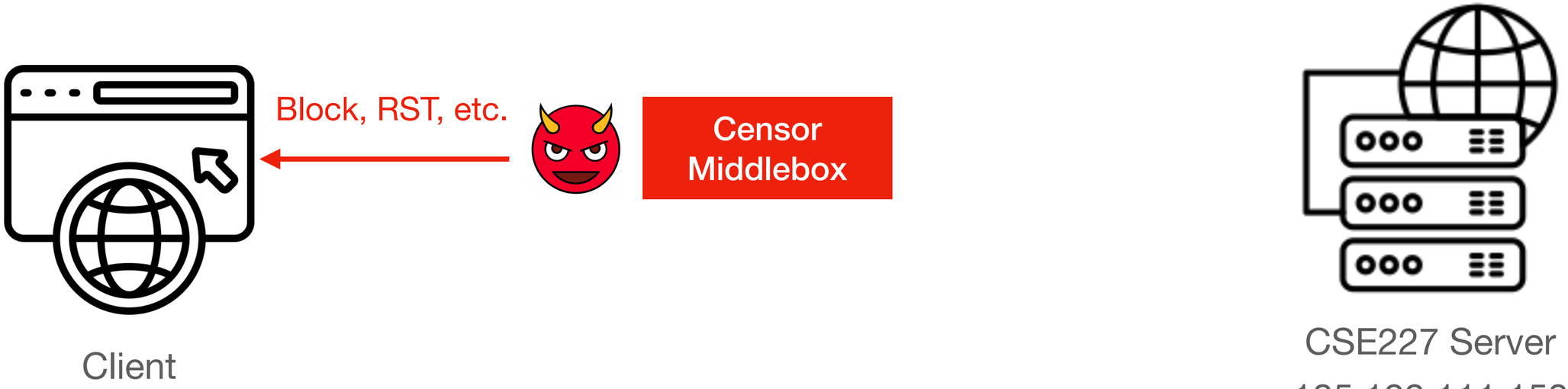
Censorship during an Internet connection

IP Blocking



Censorship during an Internet connection

IP Blocking



How easy do we think this is to implement?

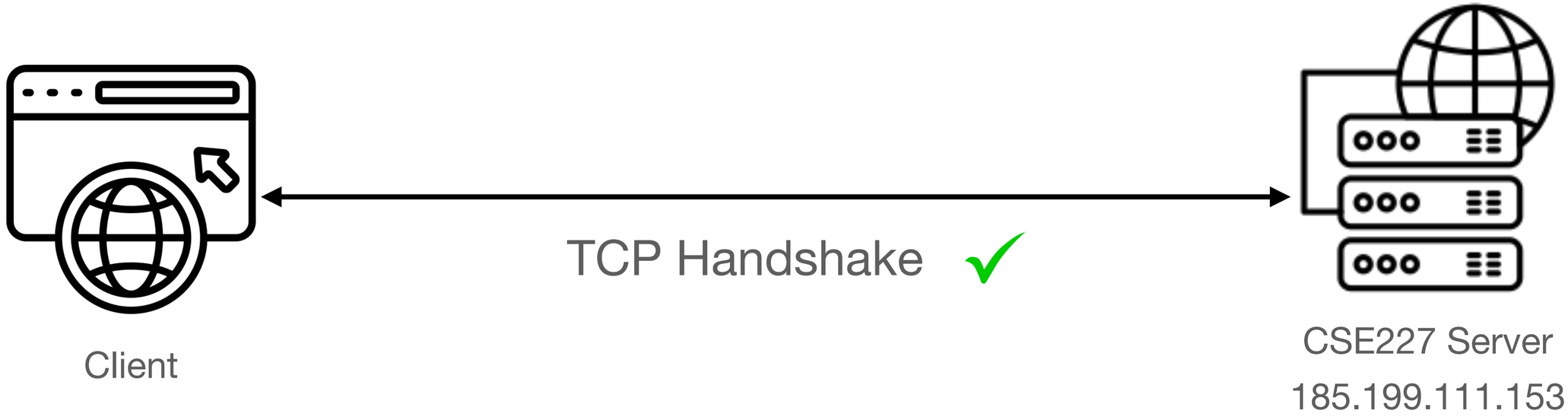
How Internet Censors Work

Major mechanisms for running Internet Censorship

- Primary form of Internet censorship: network-level blocking
- Three main ways that network-level blocking happens in practice
  - What is DNS manipulation?
  - What is IP blocking?
  - What is application layer blocking?

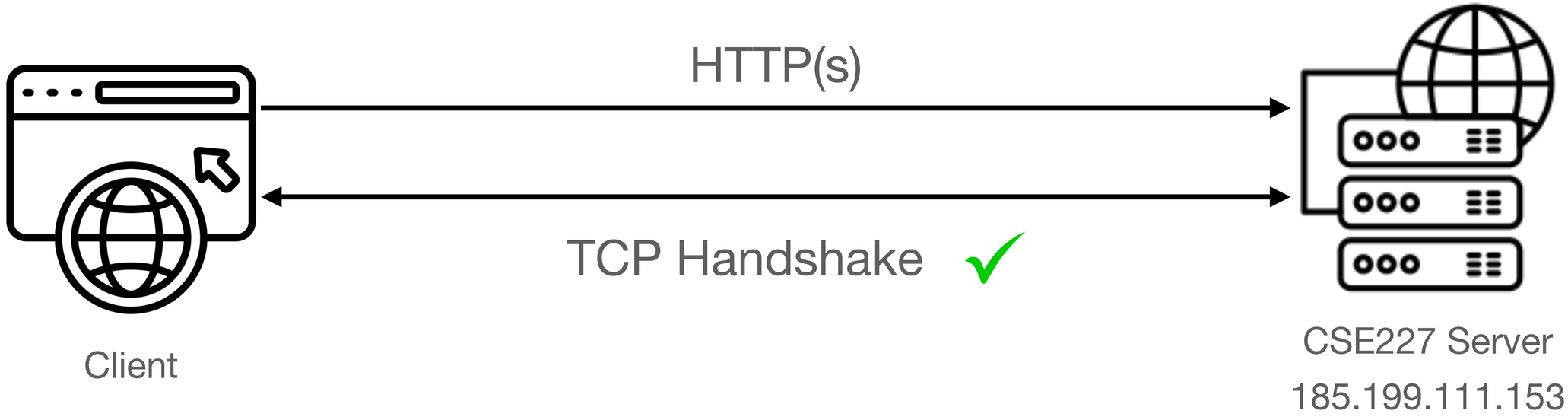
Censorship during an Internet connection

Application Layer Blocking



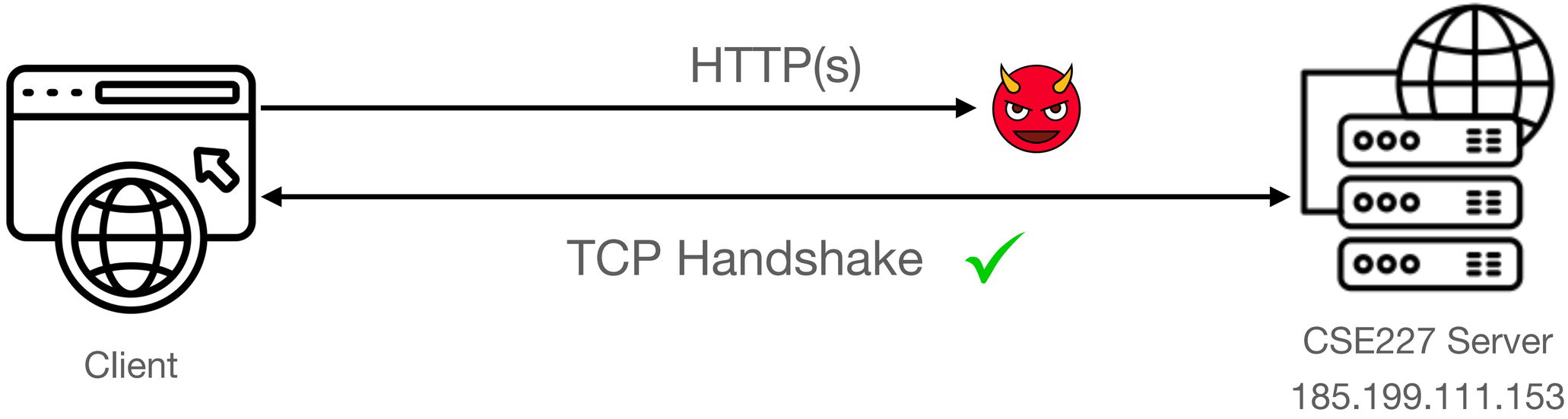
Censorship during an Internet connection

Application Layer Blocking



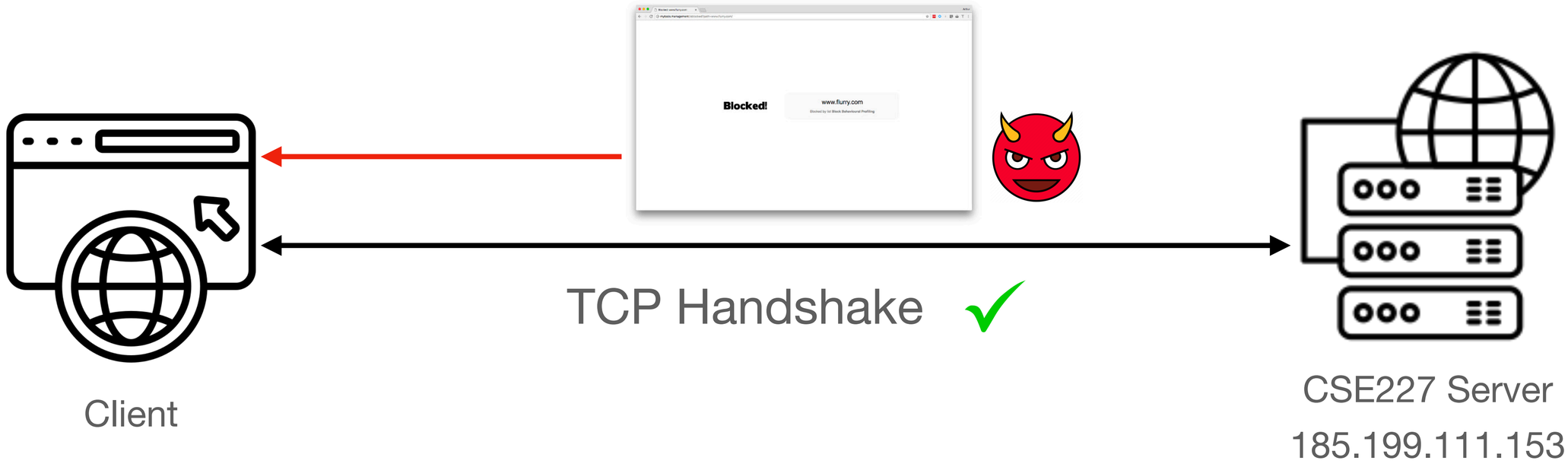
Censorship during an Internet connection

Application Layer Blocking



Censorship during an Internet connection

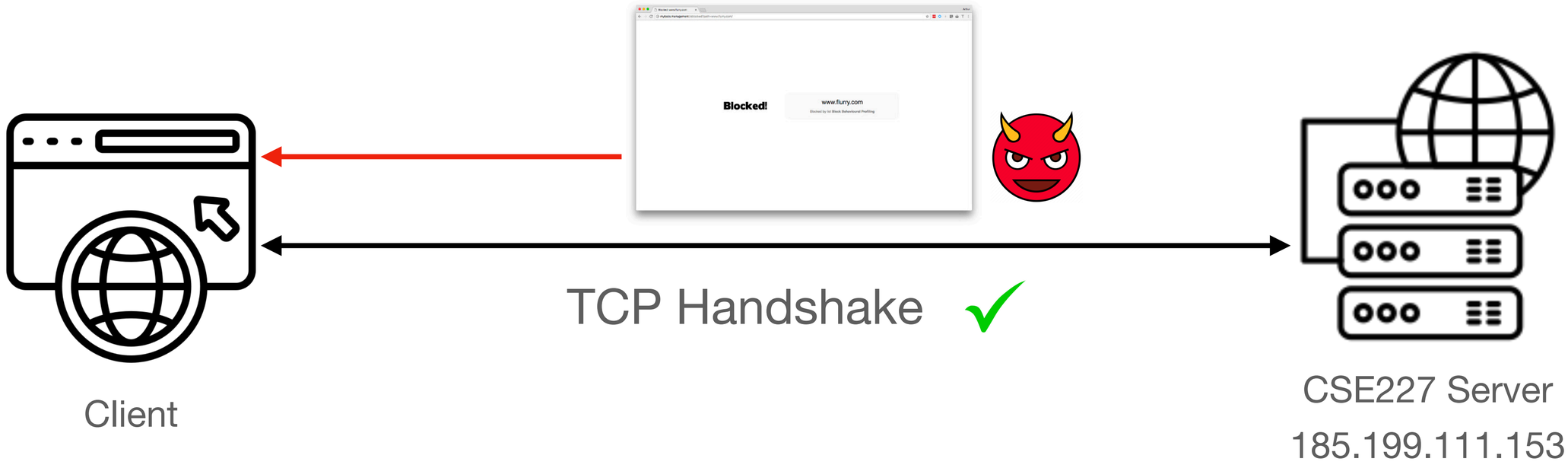
Application Layer Blocking



How easy do we think this is to implement?

Censorship during an Internet connection

Application Layer Blocking



Wallbleed

Studying China

- This paper studies what's known as the "Great Firewall of China." What is this?
- What is DNS?
- What is DNS injection?
- How does China implement DNS injection?

Studying China

- This paper studies what's known as the "Great Firewall of China." What is this?
- What is DNS?
- What is DNS injection?
- How does China implement DNS injection?
  - Through middleboxes. What is a middlebox?

Middleboxes

ad insertion

BRAS

WAN accelerator

carrier-grade NAT

transcoder

session border controller

IDS

firewall

DDoS protection

load balancer

QoE monitor

DPI

DNS Queries and Responses

- What is the Question section?
- What is the Answer section?
- What is a QNAME?
- What is RDATA?
- What do the bytes c00c mean?
- What *device* creates the Answer section?

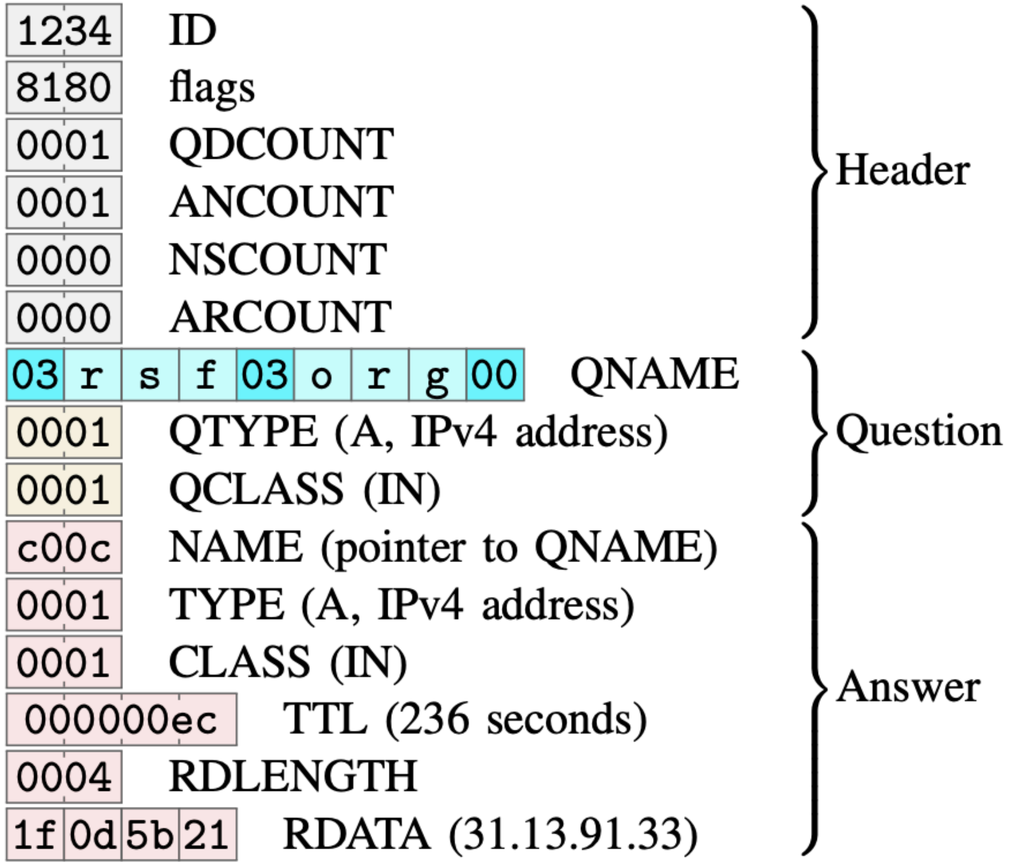


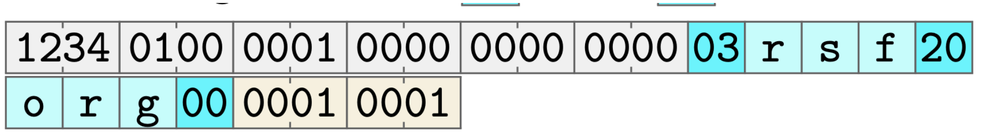
Fig. 1: The structure of an injected DNS response.

DNS Name Encoding

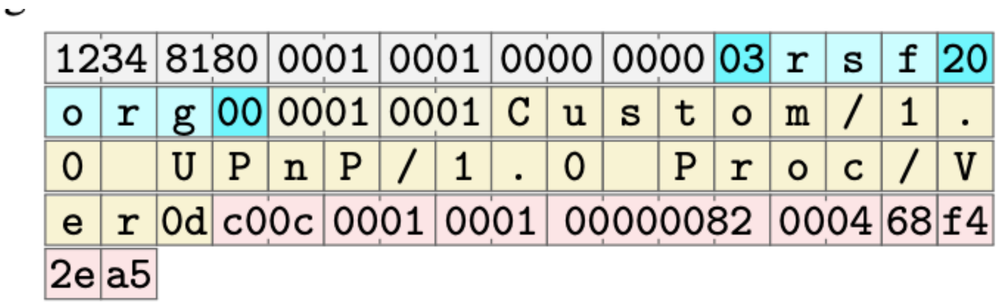
- What is a *label*?
- How are DNS names encoded in DNS packets?
- How does *Wallbleed* leverage this encoding to *leak data?*

Wallbleed

- **Poor implementation of DNS parsing leaks secret memory**
- Authors construct DNS packets where the *label length* does not correspond to the *label itself*
  - Implementation has no bounds checks, so **memory is leaked in response!**
- In this example, *~15 bytes leaked beyond the name in memory*



constructed query



response

Why does this happen?

- What do the authors posit as the reason this is happening?

Why does this happen?

- What do the authors posit as the reason this is happening?
  - DNS packets are *copied* in memory for downstream processing (e.g., checking name against a blocklist)
  - Implementers built a *custom* name parser, which doesn't perform *bounds checking*
  - So… if you control the bytes, you control how much data is returned!

What did they do…?

- Authors *exploited* Wallbleed for two years…
  - Getting 5.1B *Wallbleed responses*, GBs of data…
- Found **tons** of network protocols, architecture details, *passwords*, cookie values, secret keys….
  - You name it!
- What architecture was the middlebox running on?

Regular Expression	Note	Count	Rate
`ssdp:discover`	SSDP	184M	3.61%
`UPnP/IGD\xml`	UPnP	174M	3.41%
`(?s)[3-4]\xfttt.....-CONTROL`	(§IV-B)	121M	2.37%
`\x45\x00`	(§IV-A)	2.8M	0.05%
`uuid:WAN`	SSDP	34M	0.67%
`Host:␣`	HTTP	21M	0.41%
`(?i)Date:\s* ...`	(§IV-C)	16M	0.31%
`\x7f\x00\x00`	(§IV-D)	2.8M	0.05%
`Cookie:␣`	HTTP	2.0M	0.04%
`RCPT␣TO`	SMTP	72.5k	0.0014%
`&key=`	URL	58.1k	0.0011%
`MAIL␣FROM`	SMTP	42.4k	0.0008%
`&password=`	URL	26.9k	0.0005%

Ethics

- Do you think this research is ethical?
  - Why or why not?

Ethics

- Do you think this research is ethical?
  - Why or why not?
- Is it okay to store this data in aggregate over time?
- Is it okay to exploit a known vulnerability?
- Should the authors have disclosed this vulnerability?

Meta-thoughts

- This paper was highly contentious in discussions and remains a very divisive paper. Why?
- What about this paper *surprised* you?
- Other last thoughts?

Next time…

- Continuing in network land, we'll discuss the Cuba paper