Fair Control of the Internet: Understanding Methods, Effects and How to Know What's Being Done to Your Traffic

Presented by Allison Turner. Advised by Christine Bassem, PhD

aturner4@wellesley.edu
cbassem@wellesley.edu

WELLESLEY

DNS Manipulation [1] [2] [10]

How It Works

Every time you access a website, the domain name of the website must be resolved to a specific IP address. This address is cached for a period of time. If a client can't resolve a host name via DNS, then the client won't be able to access the content. There are two ways for this method to be executed. The first way is for a corrupted DNS server to reply to the resolution request with an incorrect IP address. The second way is for a middlebox to intercept the resolution request and reply with bad information. The client then starts requesting files from this false IP address, the incorrectly queried server will not be able to find these files, and the client will not be able to locate the content.

Detection

Content providers often direct clients to several different IPs for the same content request as a load balancing strategy, so using differnt IPs isn't always a good indicator of DNS manipulation. One team determined that DNS manipulation was present if the resolved IP was in the same service provider region as the client, or if the IP address was a specific type of faked response, called a bogon. To further determine whether these bad responses came from a middlebox or a corrupted resolver, the team ran a protocol similar to traceroute to determine whether the bad response came from the last hop of the request's routing or somewhere in between.

Network Pollution

The internet is not isolated by country. There are ways to differentiate policy based on location and service provider, but DNS requests are usually routed to the closest DNS server. One team performed DNS requests on controversial content to specific DNS resolvers around the world, and analyzed the consistency of responses. An anonymous experimenter analyzed responses to a handful of controversial domain names, and found that ~26% of responses from DNS resolvers were polluted, spanning over 109 regions.

HTTP Inspection [1]

How It Works

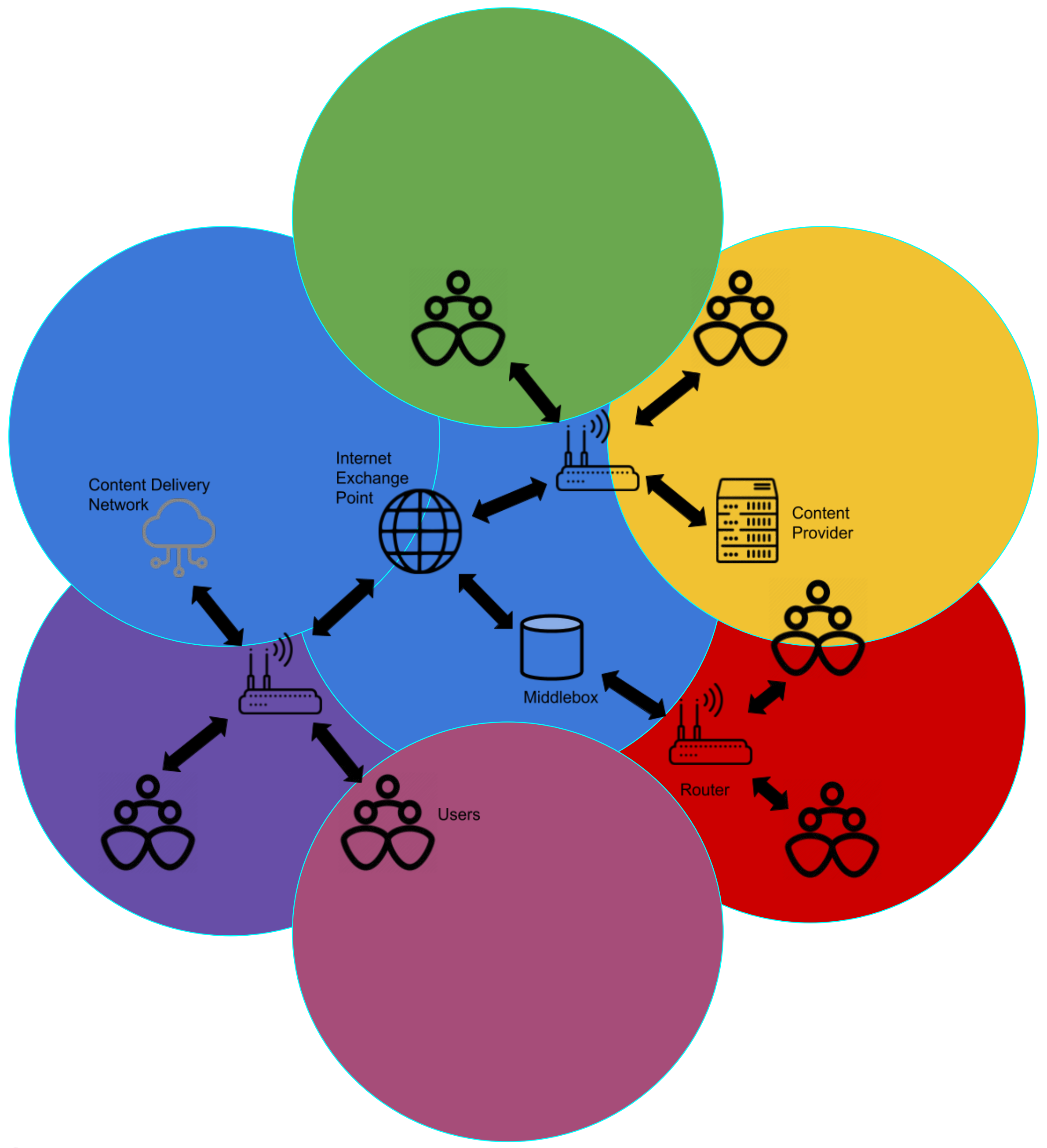
A middlebox inspects the contents of the HTTP GET request from the user. The middlebox either uses an interceptive or a wiretapping approach. An interceptive approach directly drops GET requests to censored hosts. A wiretapping approach sends a disconnection message to the user, so that the user's TCP connection is terminated, and any received information associated with that connection is discarded.

Detection

Yadav et al. describe a clear censorship/disconnection message, making the occurrence of such censorship easy to identify. The message simply terminates the TCP connection, which uses simple notifications to maintain status. The complex part of detection comes from identifying what part of the TCP handshake triggered the disconnection message. Yadav et al. used HTTP requests with iteratively larger TTL values and known censored host names. They found that interceptive middleboxes sent the disconnection message when the first TCP request message comes through, but wiretapping middleboxes send a disconnection message before the content arrives at the client, so the content still arrives but isn't registered, since the TCP connection has been terminated.

Evasion

Yadav et al. found that placing the censored host's name at an offset within the GET request and populating the Host field with a benign host evades many censors.



Differentiated Service [3] [7]

Fast Lanes, Service Limits, and More

Differentiated service is ingrained into our communications industry, seen currently in cell phone data limits and tiered internet speed plans, and debated in the fast/slow lane paradigm of non-net-neutral service providing. Many service providers achieve these business goals by first doing deep packet inspection (DPI) to determine which client the packet is associated with, what kind of data is in it if possible, and more. Providers can rate-throttle by dropping packets to trigger congestion control algorithms, give packets weighted queue priorities based on the client's usage, and defining routing rules to treat different IPs according to business priority.

Determining the Control Scheme

To determine the service level enforcement mechanism, an experiment might connect different clients with different service levels but the same computing and networking capacities to the same router. With this testbed, an experimenter would run ping trains from each client to determine any significant difference in round-trip time, to test for request de-prioritization. Next, the experimenter might test, one by one, the capacity of the router-client links by sending increasing numbers of packets, and determining any significant difference in link capacity between service levels. The experimenter could also run long-term, high-capacity, varying type jobs from a client to determine whether the service limit takes effect based on current, past, or type of activity.

BGP [6] [8] [9]

How It Works

Internet traffic does not flow in a strictly shortest-path manner; there are complex connectivity agreements between service providers to determine who will or will not share IP addresses to which they have access. BGP is the standard technical implementation of these route-sharing agreements. Implementation typically consists of sets of rules for where to forward or omit route announcements.

Methods to Infer BGP Policies

One team's approach was to set up a dozen "border routers" across several continents, to which an experimenter could attach their containerized testing framework. From such a testbed, simple tools like pings and traceroutes can reveal a lot of information. Another team uses the route-exporting patterns of neighboring routers to infer relationships. A third verifies its inferences with the sometimes-spotty Internet Routing Registry.

Potential for Network Effects

While service providers strive to deliver the fastest speeds for their customers, there is a question of how much time these access agreements add on to packet travel time, and how often BGP presents the most efficient solution. Determining these effects would require BGP policy inference, topology inference, and more.

BGP Blackholing [5]

How It Works

Internet exchange points are places where many service providers exchange traffic. (D)DoS attacks can seriously impede the efficiency of the IXP, so many IXPs filter out requests from clients who seem to be acting in an adversarial manner. Packets from filtered IPs are simply dropped as soon as the client is recognized.

Detection and Effects

Nawrocki et al. analyzed IXP traffic anomalies (ie an abnormal number of packets being dropped) within small periods of time. They found that blackholing had a collateral damage of 10^6 packets in their observed period. Obviously this affects user experience of clients significantly, requiring resent packets, which may exacerbate the classification of the client as an adversarial requestor. Collateral packets can send the experience of any application downhill, but especially some of the very applications that take up the most space in networks, ie video streaming and multiplayer gaming.

CDN Geoblocking [4]

What Is a CDN?

A Content Delivery Network is a distributed bank of servers made available to content providers to assist with user traffic load balancing. Popular CDNs include Akamai and Cloudflare. Some large companies, such as Google and Amazon, also maintain their own CDNs.

How It Works

Content providers don't want everything to be available to every user, sometimes for business reasons, and sometimes to comply with local laws. A CDN has the responsibility of not only juggling lots of customer content, but also remaining compliant with all content provider policies. CDNs provide tools to customers to define ther content/location policies, and then send 403 Forbidden (or, rarely, 451) messages to users attempting to access geoblocked content. CDNs vary on whether they explain why the content was denied.

Detection

Experimental tools can be tricky to use on commercial servers, since providers often have policies in place to prevent access by an automated tool, which often behaves like a DoSing adversary. Geoblocking tests present a resource-heavy experimental setup without a tool to spread traffic to different countries, like with Luminati. Once these hurdles have been crossed, one only needs to request a web page from a client machine to observe the result.

Future Work

The purpose of investigating these methods of network manipulation was to study the authors' experimental setups for determining control policies and schemes. We intend to use this assembled knowledge to build a tool that can measure and detect such policies and schemes.

[1] "Where The Light Gets In: Analyzing Web Censorship Mechanisms in India" by Yadav et al. IMC '18, October 31-November 2, 2018, Boston, MA, USA.
[2] "Global Measurement of DNS Manipulation" by Pearce et al. Proceedings of the 26th USENIX Security Symposium, August 16-18 2017, Vancouver, BC, Canada.
[3] "Enabling Fast and Slow Lanes for Content Providers Using Software Defined Networking" by Gharakeili et al. IEEE/ACM Transactions On Networking, November 29 2016.
[4] "403 Forbidden: A Global View of CDN Geoblocking" by McDonald et al. IMC '18, October 31-November 2, 2018, Boston, MA, USA.
[5] "Down the Black Hole: Dismantling Operational Practices of BGP Blackholing at IXPs" by Nawrocki et al. IMC '19, October 21–23, 2019, Amsterdam, Netherlands.
[6] "On Inferring and Characterizing Internet Routing Policies" by Wang and Gao. IMC'03, October 27–29, 2003, Miami Beach, Florida, USA.
[7] "Not Paying the Truck Driver: Differentiated Pricing for the Future Internet" by Trossen and Biczók. ACM ReArch 2010, November 30, 2010, Philadelphia, USA.
[8] "High-Fidelity Interdomain Routing Experiments" by Junior et al. SIGCOMM Posters and Demos'18, August 20–25, 2018, Budapest, Hungary.
[9] "Intent-based Analysis of Network-wide Routing Policy Configuration" by Levanti et al. INM'07, August 27–31, 2007, Kyoto, Japan.
[10] "The Collateral Damage of Internet Censorship by DNS Injection " by Anonymous. ACM SIGCOMM Computer Communication Review 22 Volume 42, Number 3, July 2012.