Internet 202: Why All The Fuss About Hacking the DNS?

Dr. Eric W. Burger

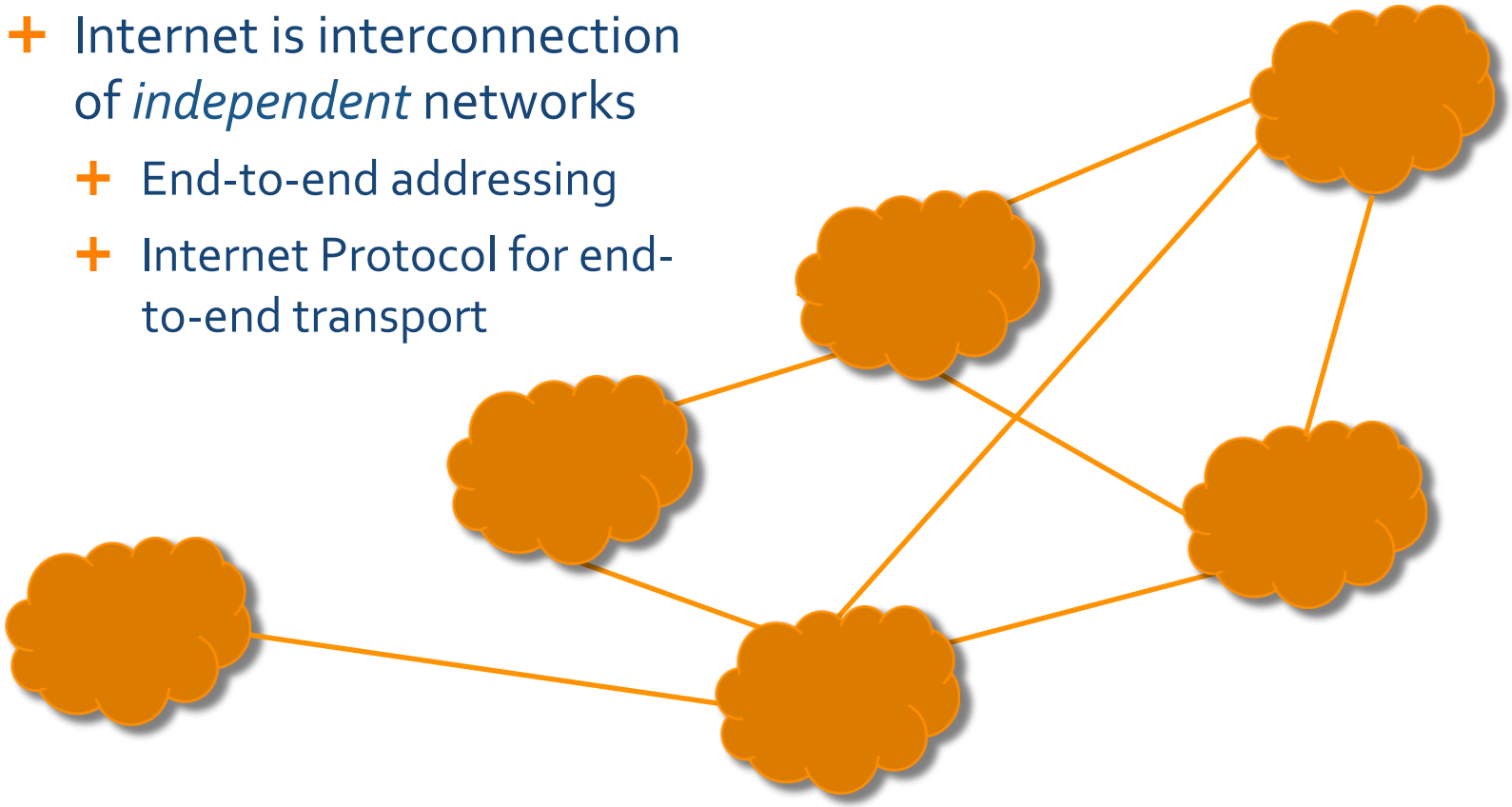
ABA Committee 355 - 2/21/12

Disclaimer – I Am Not Speaking On Behalf Of:

- Georgetown University (Faculty)
- Internet Society (Trustee)
- Internet Engineering Task Force (Trustee)
- IEEE/IEEE-USA
  (Past Chair, Committee on Communications Policy)
  (Chair, Joint CCP/Intellectual Property Committee Work Group on IPR and Piracy)
- SIP Forum (Chairman Emeritus)
- ICANN/PIR/or other I* organizations

Review from Internet 201

- Internet is interconnection of *independent* networks
  - End-to-end addressing
  - Internet Protocol for end-to-end transport



http://www.standardstrack.com/StandardsTrack_Eric_Burger/Speeches_and_Articles/Entries/2011/2/7_Internet_201__The_DNS_and_IPR.html

Internet Applications

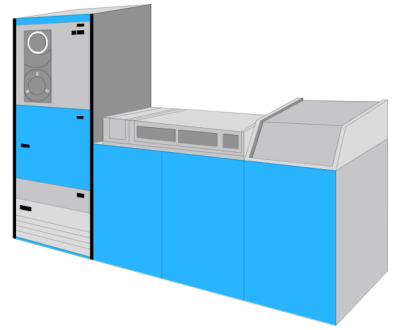
- WWW, Email, Jabber, SIP, FTP, Torrent, Seti@Home, …

Foundational Principles of the Internet

- Dumb network, smart endpoints
  - Network is ignorant of the application
  - Network job is routing (delivery) of packets
- New applications do not require network modifications
- New applications do not need permission from the network operator
- Trade inefficient allocation of reserved resources for efficient transport of packets
  - Optimization requires application knowledge
  - 35 years of experience has proven this model

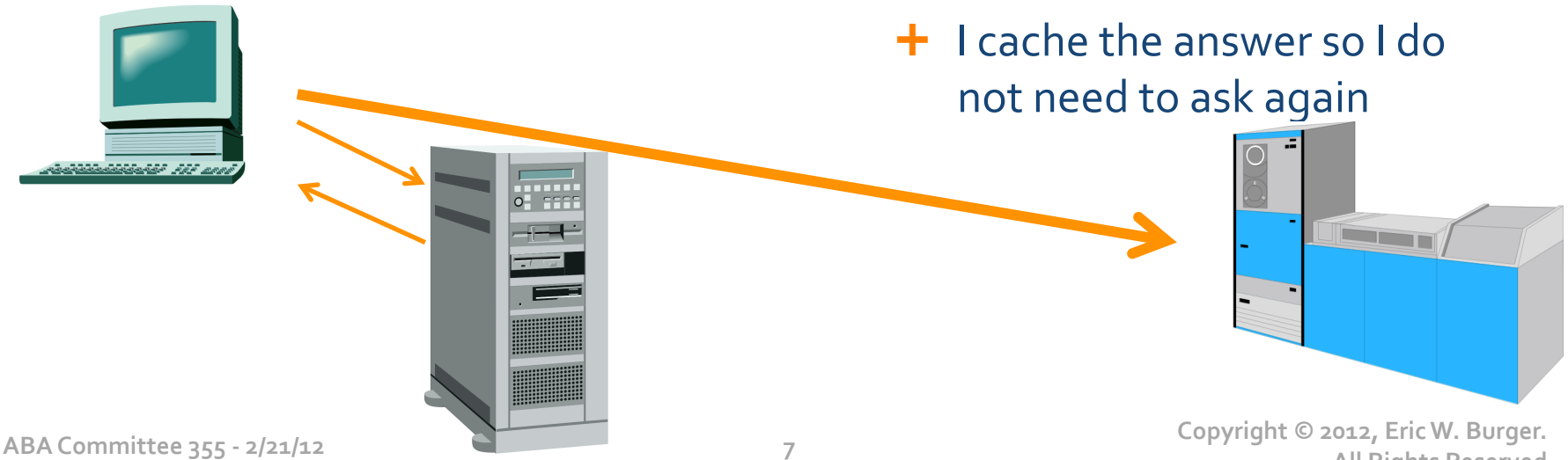
How Does the DNS Work?

- Where is www.georgetown.edu?
- Do I know where it is?
- Check my local cache (my DNS Resolver)
- If I have address, I go directly to the server



How Does the DNS Work?

- I don't know where it is…
- My computer asks my ISP's Caching DNS Server if they know where it is
- If they do, great
  - I go directly to the host
  - I cache the answer so I do not need to ask again



How Does the DNS Work?

- My ISP does not know the IP address
- DNS Recursive Server searches for the answer

Where is www.**georgetown.edu**

Root DNS Server

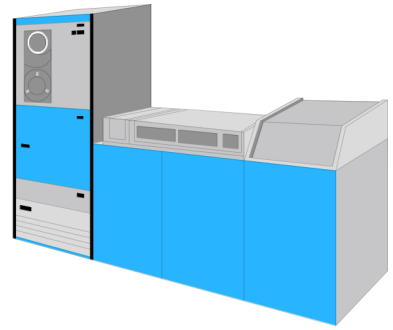
.EDU Authoritative Server

ISP Recursive Server

Georgetown Authoritative Server

How Does the DNS Work?

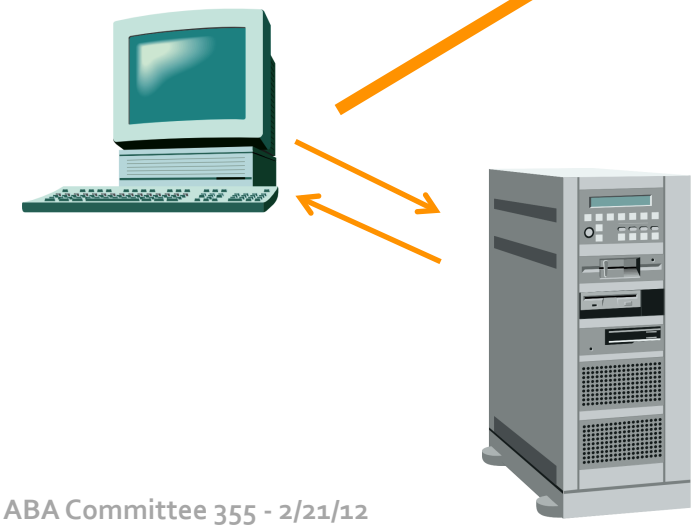
- Now I know where www.georgetown.edu is
- ISP DNS Cache stores
  - .EDU
  - georgetown.edu
  - www.georgetown.edu
- I cache
  - www.georgetown.edu



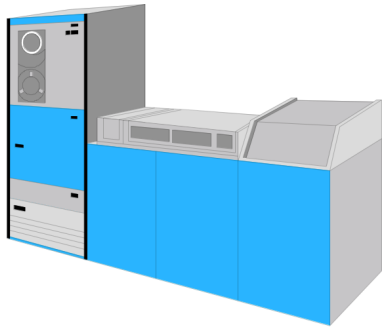
Attacks on the DNS

- Cache poisoning
  - Force fake update of IP address to ISP's DNS Cache

www.georgetown.edu
192.220.74.179
(a.k.a. badplace.ru)

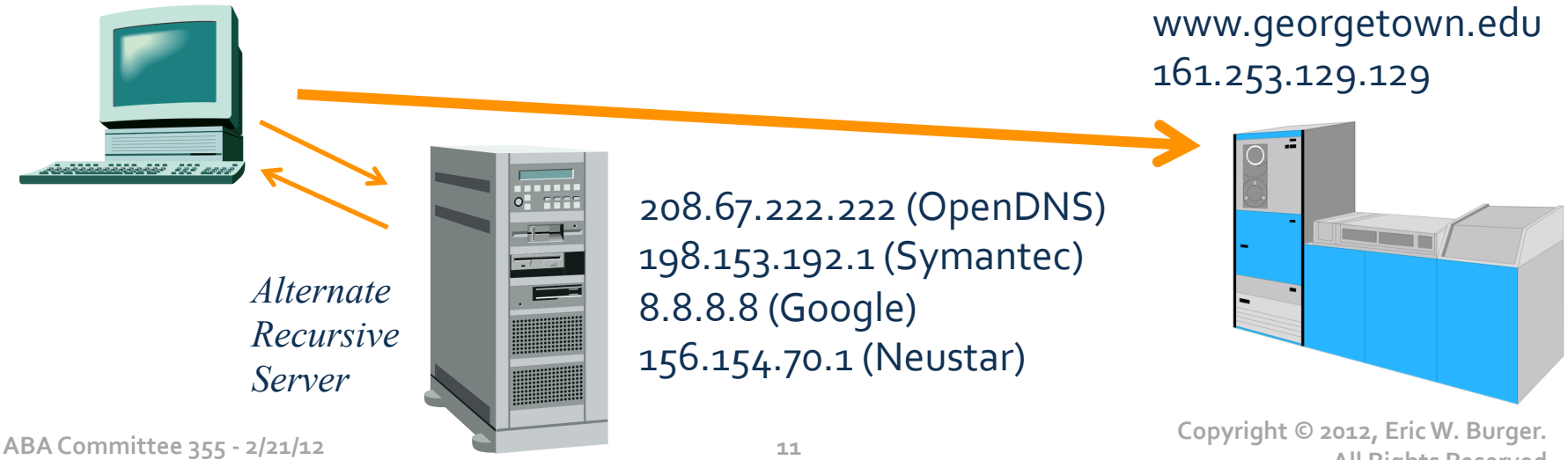


www.georgetown.edu
161.253.129.129



Attacks on the DNS

- Alternate DNS Recursive Server
  - Why? Much faster than ISP's DNS Cache; Avoid broken caches offering "help"; route around failures



Attacks on the DNS

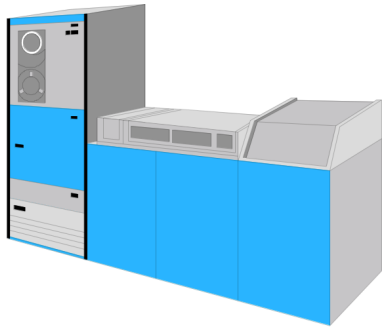
- Alternate DNS Root
  - Why? Ideology and/or compete with ICANN; route around failures

www.georgetown.edu
192.220.74.179
(a.k.a. badplace.ru)

Alternate Recursive Server

Name.Space
NewNations
OpenNIC
BadEvilDude

www.georgetown.edu
161.253.129.129



Avoid Evil: DNSSEC

- Root is signed
- TLD Authoritative server signed, signs for domains
- Domain Authoritative server signed, signs for subdomains

Root DNS Server

.EDU Authoritative Server

End-to-End Integrity Validation

ISP Recursive Server

Georgetown Authoritative Server

How To Do a "Take Down"

- ICE gets registrar to change registration of domain to point to ICE
- ICE returns ICE's server IP address

Root DNS Server

.COM Authoritative Server

ISP Recursive Server

ICE Authoritative Server

Takedowns Work

- Literally a taking of the domain name
- Domain name resolves to ICE
- Issues
  - Unless servers seized, servers still reachable
  - Only works for U.S.-based registrars
  - Can also work for U.S.-based registries
  - Trivial to get new U.S. domain and non-U.S. TLDs

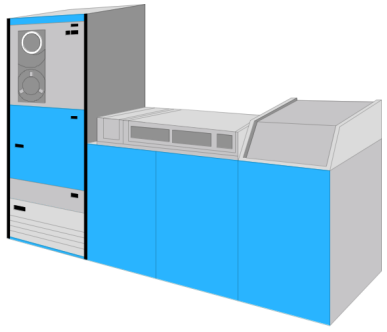
rojadirecta.org ➔ .com ➔ .es

DNS Filtering

- Instead of taking domain name at registry, make ISP lie about address
- Works no matter where registry is

ISP Caching Server

Illegalplace.co.uk



What Could Go Wrong With DNS Filtering?

- Big issue is one cannot tell why answer was changed
  - Was ISP was under court order?
  - Is ISP being evil?
  - Is an evil third-party being evil?
- We do have an answer for this: DNSSEC
  - DNSSEC provides integrity and security of the responses in the DNS

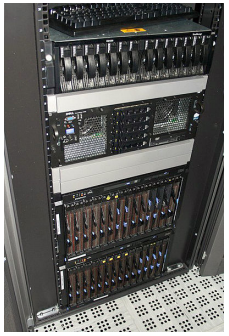
DNSSEC Integrity

- Deals with rogue Recursive Server
- Deals with cache poisoning
- Detects any change from target Authoritative Server to me

Root DNS Server

.EDU Authoritative Server

ISP Recursive Server



Georgetown Authoritative Server

What Happens When ISP Lies?

- Record will fail integrity check
  - Probably not signed by TLD
  - Definitely not signed by domain being resolved
- Impossible to tell record is not an attack on the DNS
- What about just not doing DNSSEC to user
  - This is known as a downgrade attack
  - Best: Users configured to reject unsigned DNS responses
  - Worst: Users call their ISP asking about weird DNS behavior
  - Results in ISPs not deploying DNSSEC
- What about returning a new error code, like "Censored Domain"?
  - Cannot be signed by domain, for obvious reasons
  - Another downgrade attack: whitehouse.gov could get "Censored Domain" response

Why Do We Care About DNSSEC?

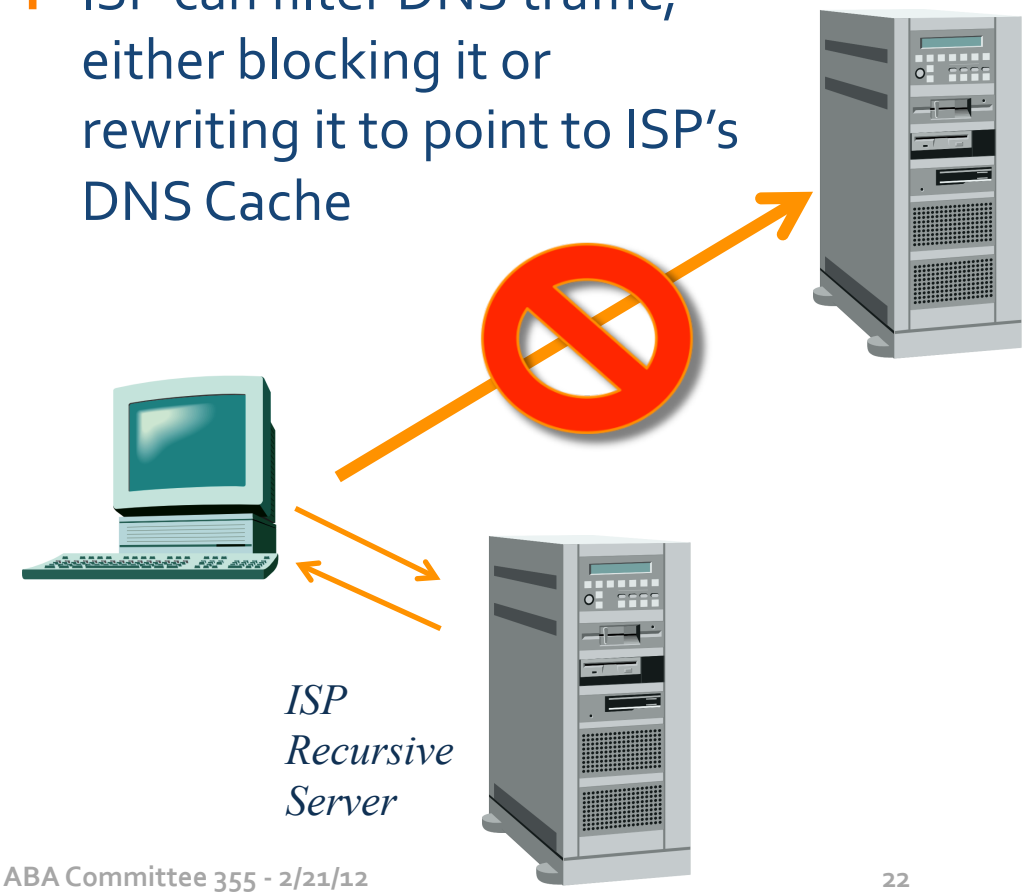
- Recall all the evil cases
- DNSSEC addresses many of the evil cases
- Impossible to differentiate an attack from a takedown
- Society needs to decide if protection from bank fraud, identity theft, terrorist funding, theft of corporate data, etc. is less important than COICA, SOPA, PIPA, TPP, or ACTA's stated goals

What If DNSSEC "Fixed"?

- Trivial for user to go to alternate DNS service
  - May be legitimate service
  - Would most likely follow U.S. laws if in U.S.
  - Would most likely drive users outside U.S.
  - Strong potential for bad actors to be in DNS Resolver business
  - Encourages bank fraud, identity theft, terrorist funding, theft of corporate data, etc.
- Some regimes have policy measures to address use of alternate DNS servers

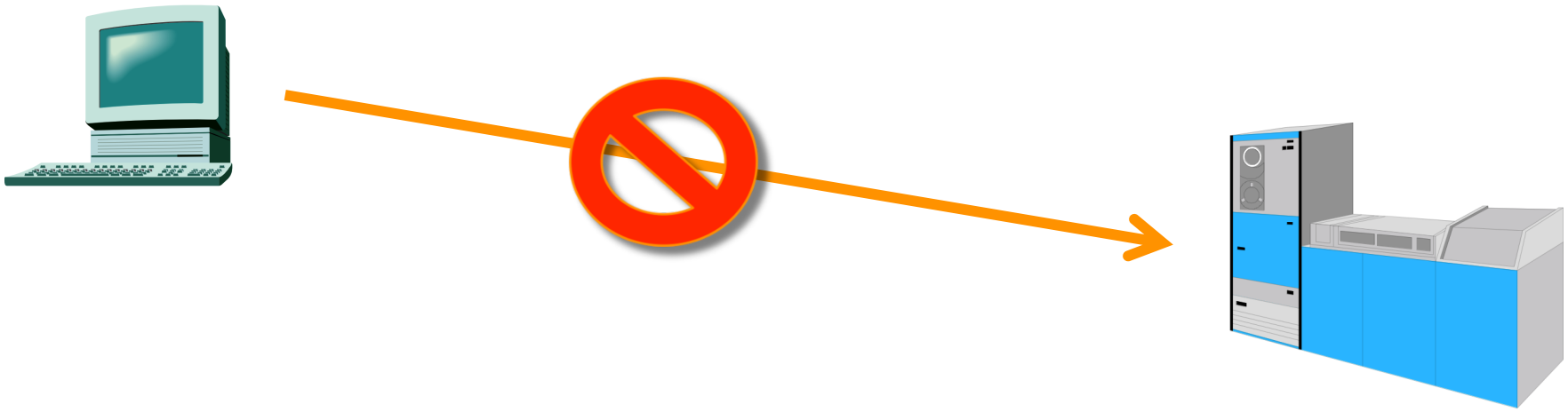
DNS Blocking

- ISP can filter DNS traffic, either blocking it or rewriting it to point to ISP's DNS Cache



Inverse Firewall

- ISP can filter traffic to banned IP addresses



What is Wrong With Blocking?

- Very successfully used in People's Republic of China, Iran, Oman, Saudi Arabia, and other countries
- Requires deep packet inspection
  - Wiretap on ALL user communication
  - Arms race:
    - Encapsulated protocols
    - Encrypted channels

Issue For the Policy Community

- The Internet is the interconnection of independent networks
  - No one needs permission to create an application
  - Network supports innovation, without needing to upgrade network
  - Greatest medium since writing for getting ideas disseminated
- Requirements for all protocols, especially since 2003 (RFC3552), include
  - Security considerations
  - End-to-end integrity considerations
  - Denial of service avoidance
- The Internet's basic construction avoids censorship
  - Successfully used to restore human rights, restoring freedom of speech, assembly, and self-determination

Is this not the goal of American domestic and foreign policy?

We hold these truths to be self-evident, that all men are created equal, that they are endowed by their Creator with certain unalienable Rights, that among these are Life, Liberty and the pursuit of Happiness.