DNS Analysis and Threats in IPv6 Automatic Transition Mechanisms

based on work under submission

John Kristoff

DePaul University (ops role)
University of Illinois at Chicago (research role)

jtk@depaul.edu

In collaboration with:

Chris Kanich <ckanich@uic.edu>
Jason Polakis <polakis@uic.edu>
Mohammad Ghasemisharif <mghas2@uic.edu>

Agenda

- Research summary
- IPv6 Automatic Transition Mechanisms Overview
- ISATAP registered names, auth servers, queries
- View from the resolvers and root servers
- ISATAP relay router recap
- Epilogue

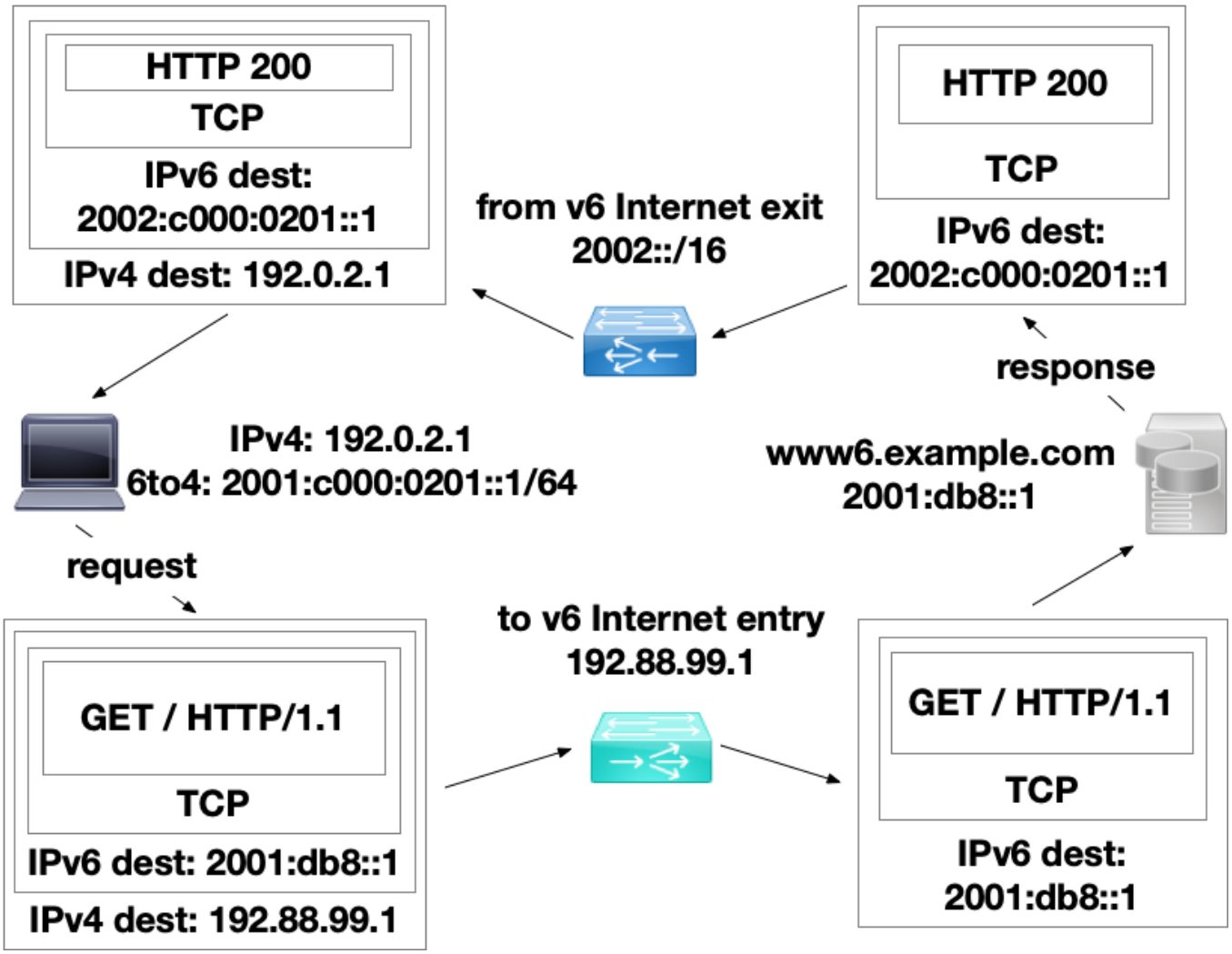
Security Implications

- The Folly of IPv6 Automatic Transition Mechanisms
- Traffic hijacking threats due to:
  - DNS name capture
  - Route capture
- Additional threats include:
  - Source address spoofing
  - Denial-of-service
  - Infrastructure disclosure
  - Policy bypass

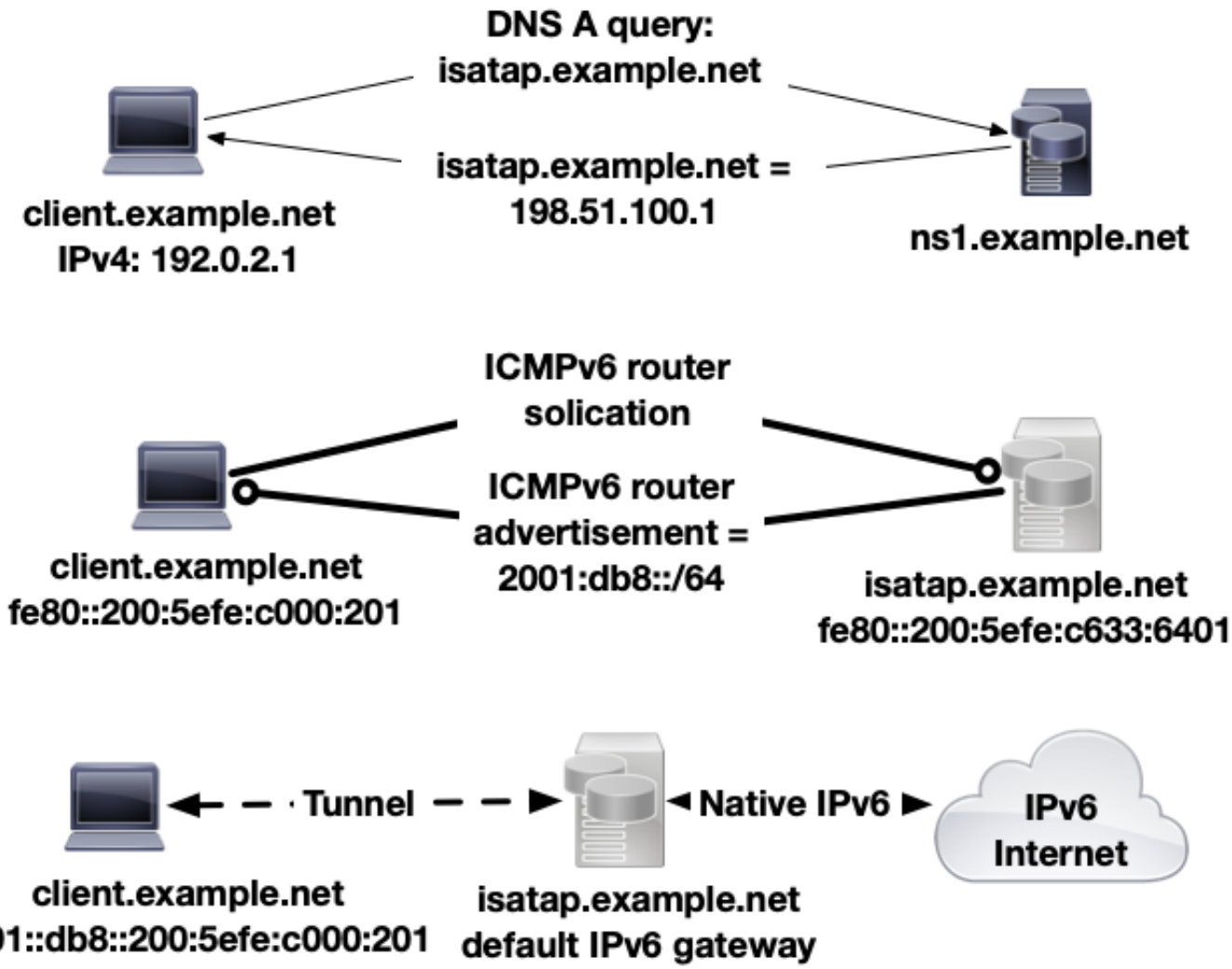
Experiments and Data Analysis

- Domain name registrations
- BGP route announcements
- Open tunnel relays
- Auth, resolver, root server query measurements
- Controlled ISATAP relay

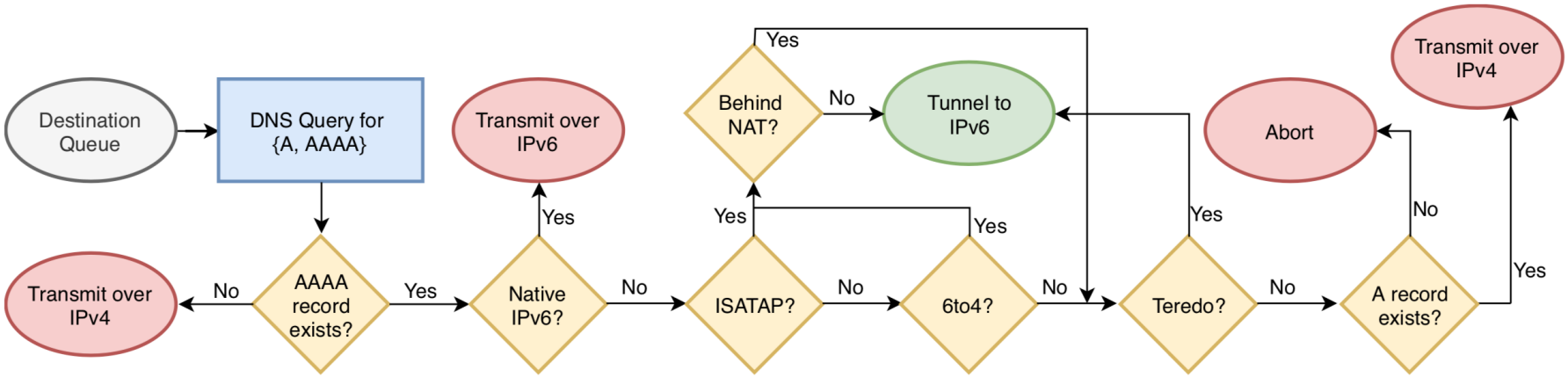
6to4


HTTP 200
TCP
IPv6 dest:
2002:c000:0201::1
IPv4 dest: 192.0.2.1
from v6 Internet exit
2002::/16
HTTP 200
TCP
IPv6 dest:
2002:c000:0201::1
response
IPv4: 192.0.2.1
6to4: 2001:c000:0201::1/64
www6.example.com
2001:db8::1
request
to v6 Internet entry
192.88.99.1
GET / HTTP/1.1
TCP
IPv6 dest: 2001:db8::1
IPv4 dest: 192.88.99.1
GET / HTTP/1.1
TCP
IPv6 dest:
2001:db8::1

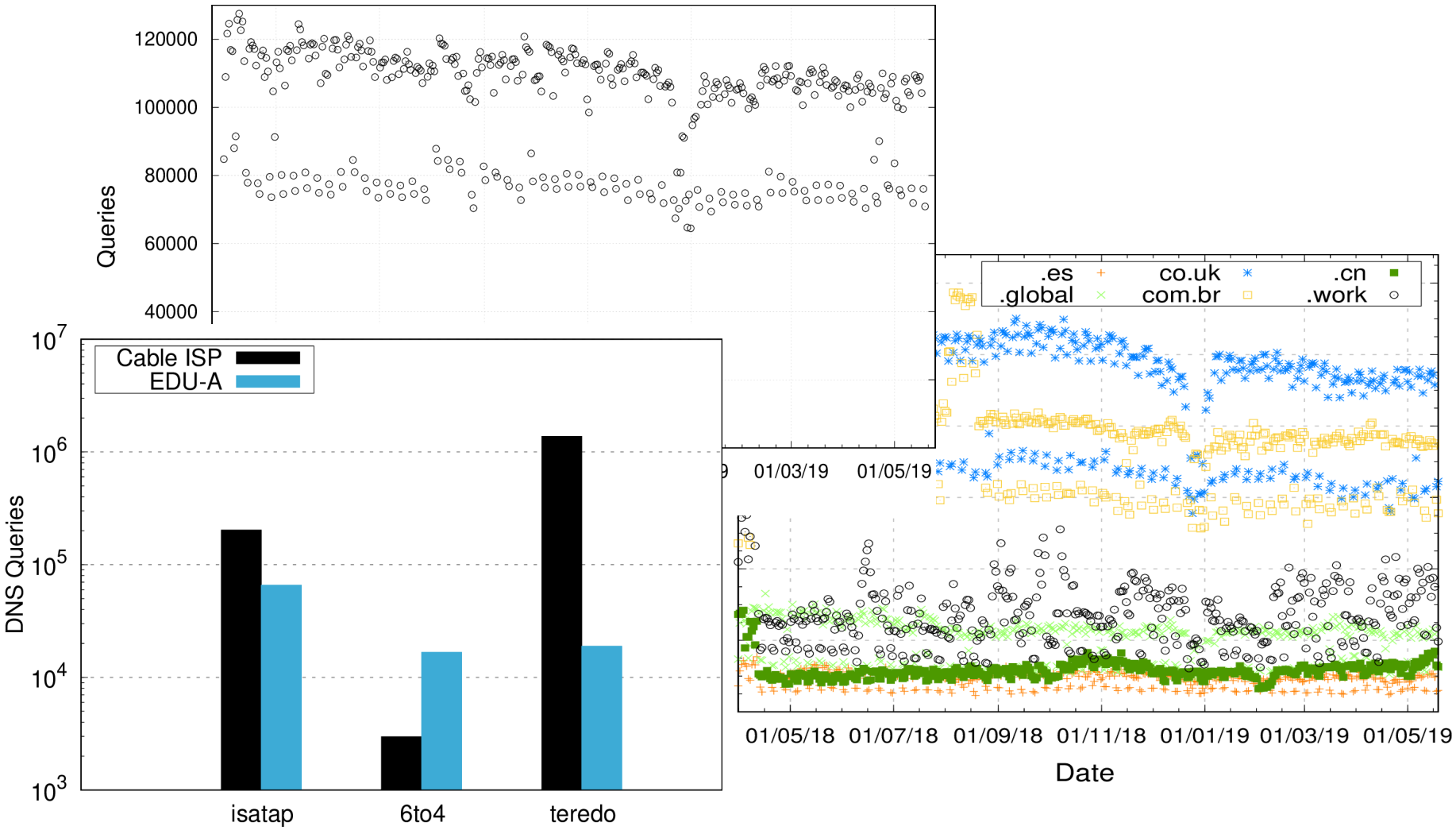
ISATAP


DNS A query:
isatap.example.net
isatap.example.net =
198.51.100.1
client.example.net
IPv4: 192.0.2.1
ns1.example.net
ICMPv6 router
solication
ICMPv6 router
advertisement =
2001:db8::/64
client.example.net
fe80::200:5efe:c000:201
isatap.example.net
fe80::200:5efe:c633:6401
Tunnel
Native IPv6
IPv6
Internet
client.example.net
2001::db8::200:5efe:c000:201
isatap.example.net
default IPv6 gateway

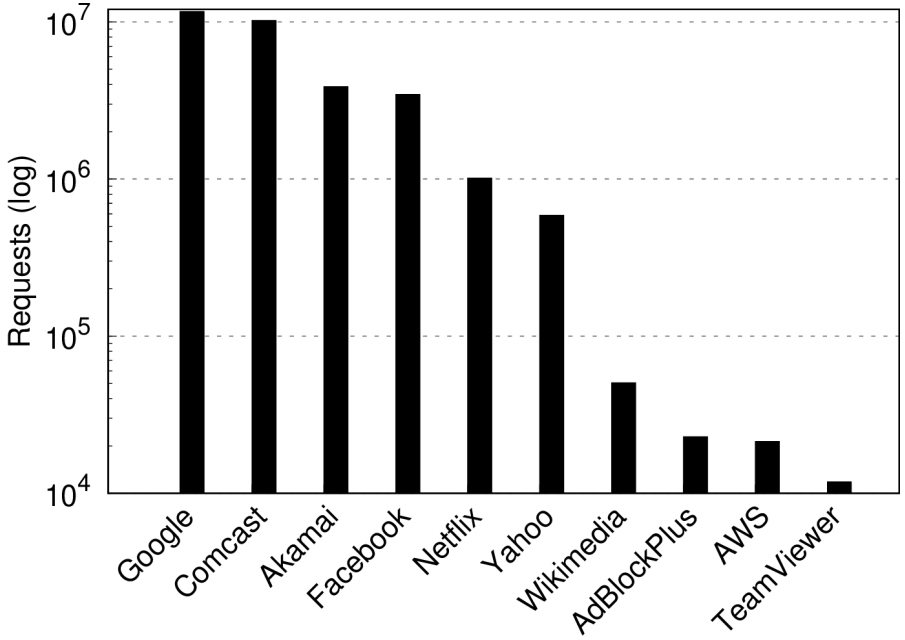
Mechanism Selection Summary

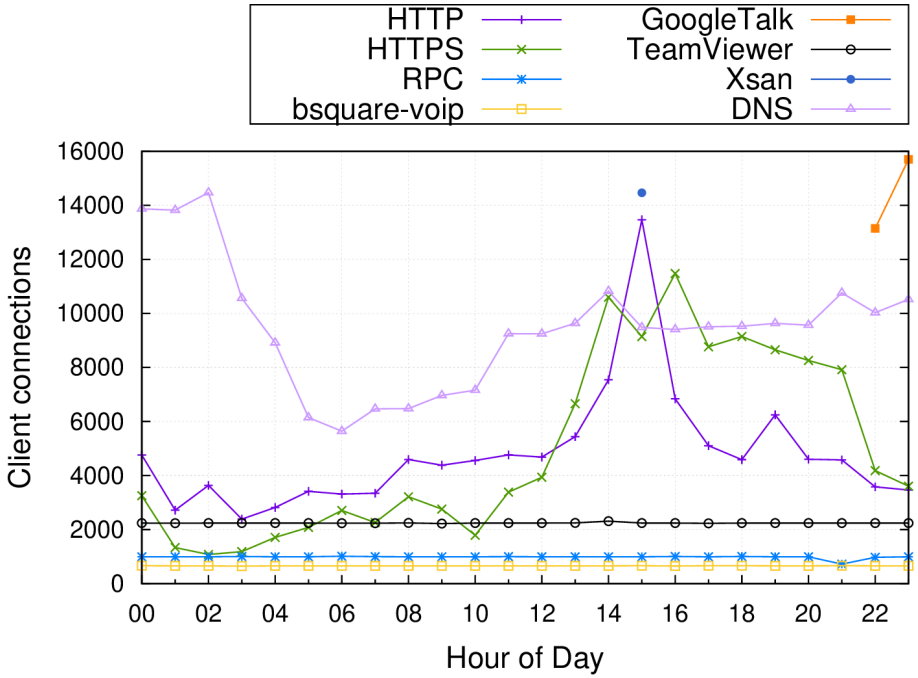


IPv6 Automatic Transition: names, servers, and queries



ISATAP Relay Experiments





ECS-enabled Logging

- 2404:6800:4008:c05::111<-**61.139.113.0/24** wants 'isatap.tech|A', do = 1, bufsize = 1680: packetcache MISS
- 173.194.91.67<-**2804:7f7:db80:8e00::/56** wants 'isatap.com.br|A', do = 1, bufsize = 1680: packetcache MISS
- 183.232.126.140<-**111.230.66.1/32** wants 'isatap.xyz|A', do = 1, bufsize = 1680: packetcache MISS

Epilogue

- Hard code label prefixes considered harmful?
- Name and route coupling challenges
- Loosely (nonexistent) authenticated provisioning
- ISATAP registrations
- [6to4,teredo].ipv6.microsoft.com do not resolve
  - But gets a lot of queries

  Related to name collision discussions in ICANN
- Lessons for DoH canaries?

Contact Info

- John Kristoff
- Email: jtk@depaul.edu
- WWW: https://aharp.iorc.depaul.edu
- GitHub: https://github.com/jtkristoff
- Twitter: https://twitter.com/jtkristoff