

# naycast

- Anycast exploration
  - (A five minute talk)

# Who am I?

- Jacob Appelbaum
  - <[jacob@appelbaum.net](mailto:jacob@appelbaum.net)>
- I like to take pictures (of people and networks)
  - I dislike slide presentations

# Examining anycast networks

- How to find otherwise obscured but useful information about a network at the application layer

# What is anycast?

- Injecting routes from multiple locations
- An example?
  - Nodes located around the world all announcing the same IP space
    - Nyc, Tokyo, Paris, San Francisco
  - How does it work?
    - BGP does all the routing magic
- What is it useful for?
  - high availability
    - seamless fail over
    - localized nodes

# Popular applications

- Web servers (TCP failure rate of 1 in 10,000)
- DNS servers

# Subverting the application

- Why?
  - Find back channels

# How about webservers

- Are they properly configured?
  - What does that mean anyway?

# How about DNS?

- Recursive DNS?
  - Sounds nice, lets roll some packets

# Blind attack

- Spoof your source address
  - Keep track of it
  - Set your request to contain a reversible encoding of your source address
    - Keep each request unique to prevent caching and force lookups
  - Send it and forget

# Watch replies

- Run the auth DNS and parse logs
  - (or sit upstream from it and monitor)
- Correlate the requests

# Important things to note

- Is it a unicast node making the query?
- Repeat the query (with the same source)
- Learn about the upstream routing configuration across the cluster
  - per packet load balancing?
  - per source address?
  - How does it behave?
  - Does it stick? Does it shift?

# Count the unicast nodes

- Same address space as the anycast nodes?
- Did you discover some other ip space?
- How many nodes in total?

# Take it further

- Once you know the upstream routing configuration...
  - Does the discovered backend IP space have the same transit?
    - Unicast nodes present a much more certain path to a given “cluster”
    - Location specific attacks are undampened by anycast routing
  - Fingerprinting services and specific node state
  - “Hot or Not?”
    - See sjmurdoch's paper from the 23c3

# Code

- cloudburst
  - Available later tonight

# Questions?

- (Thanks to David Molnar, grey-, h1kari, Dan Kaminsky, Xley)