Network Telescopes

David Moore

September 23rd, 2003

DIMACS Large-scale Internet Attacks Workshop

dmoore @ caida.org

www.caida.org

www.cs.ucsd.edu

UCSD CSE

caida

Outline

- What is a network telescope?
- Does size matter?
- Distributed telescopes
- Anycast telescopes
- Transit telescopes
- Honeyfarms
- Conclusions

Network Telescope

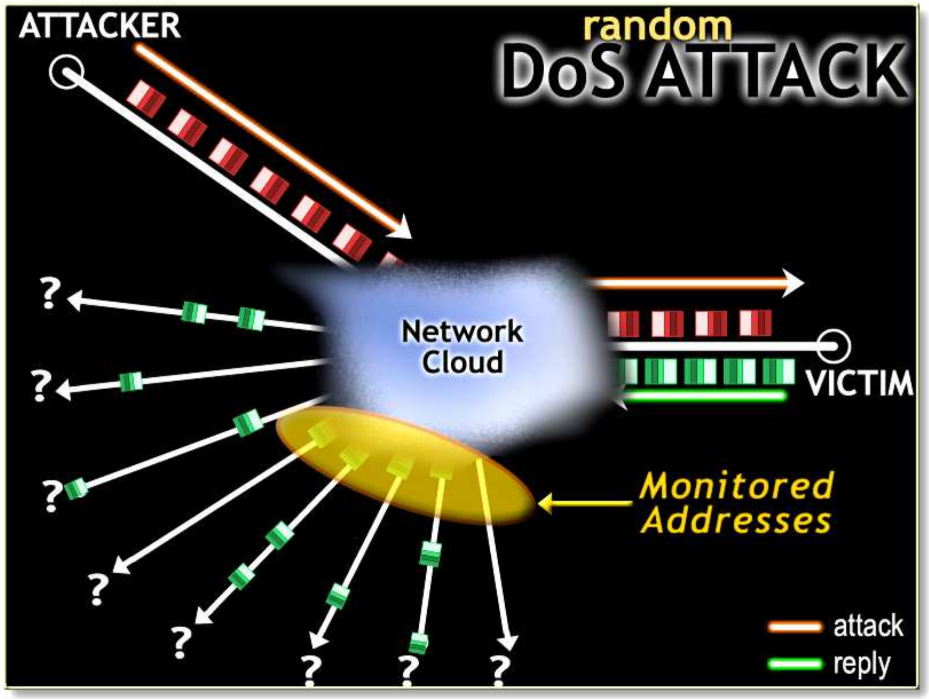
- Chunk of (globally) routed IP address space
- Little or no legitimate traffic (or easily filtered)

- Unexpected traffic arriving at the network telescope can imply remote network/security events

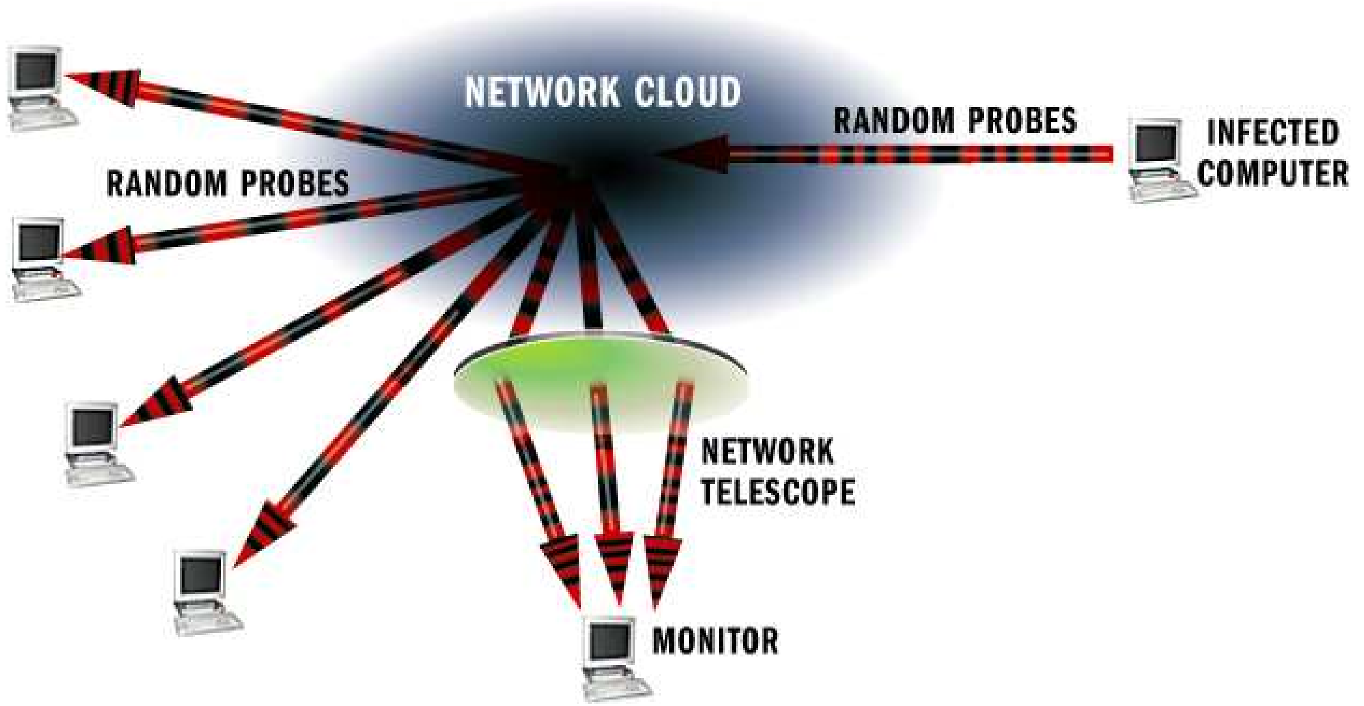
- Generally good for seeing explosions, not small events
- Depends on statistics/randomness working

Network Telescope: Denial-of-Service Attacks

- Attacker floods the victim with requests using random spoofed source IP addresses
- Victim believes requests are legitimate and responds to each spoofed address
- With a /8, one can observe 1/256th of all *victim responses* to spoofed addresses



Network Telescope: Worm Attacks



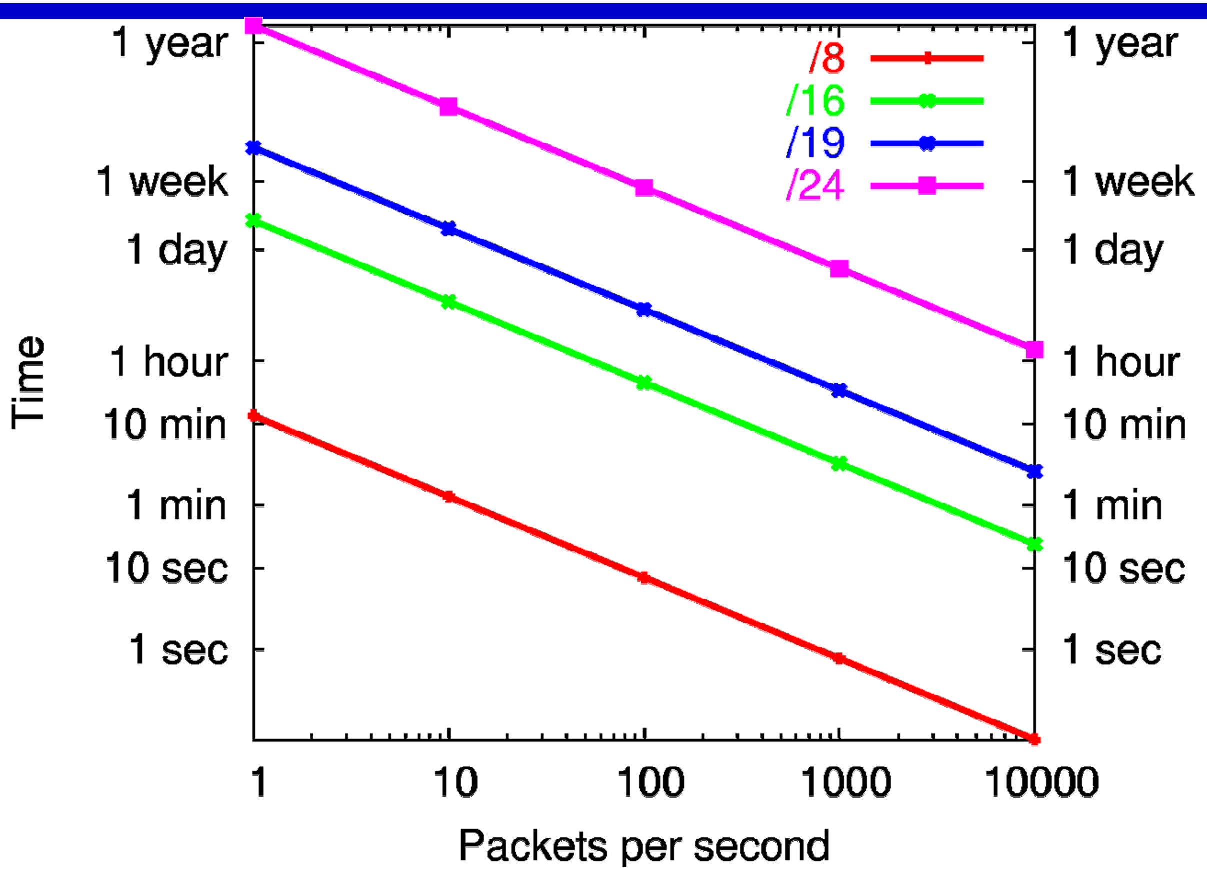
- Infected host scans for other vulnerable hosts by randomly generating IP addresses
- A /8 monitors 1/256th of all IPv4 addresses
  - 1/256th of all *probes* of worms (with no bias and no bugs)

Does size matter? – Yes.

- Larger telescopes are able to detect events that generate fewer packets, either because of short duration or low sending rate.

- Larger telescopes have better accuracy at determining the start and end times of an event.

Detectable Events (95%)



Any event above and to the right of a line can be detected (at least one packet seen) with at least 95% probability.

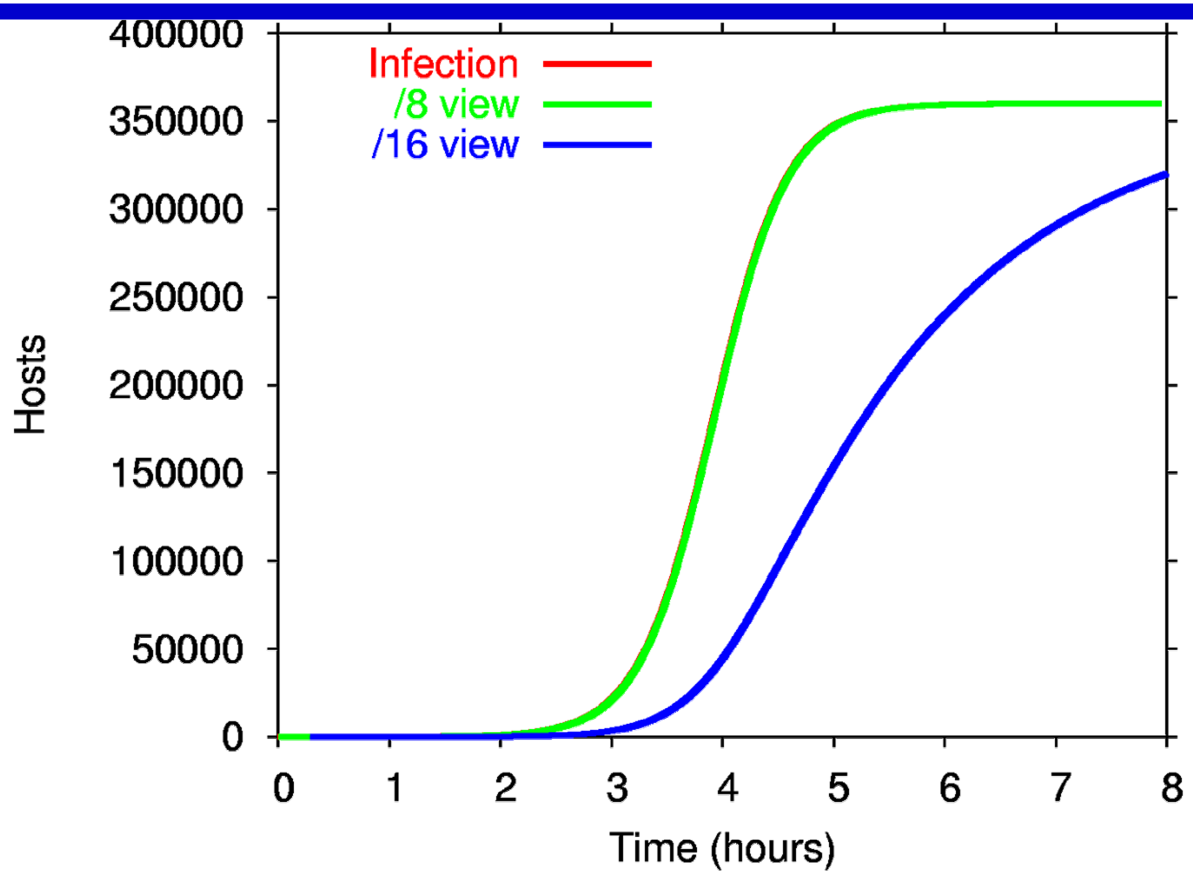
Detection Times - 10 pps events

(Code-Red approx. this rate)

Detection probability:	5%	50%	95%
/8	1.3 sec	18 sec	1.3 min
/14	1.4 min	19 min	1.4 hour
/15	3 min	38 min	2.7 hour
/16	6 min	1.3 hour	5.5 hour
/19	45 min	10 hour	1.8 day
/24	24 hours	14 day	58 day

Worm Spread – 10 probes/sec

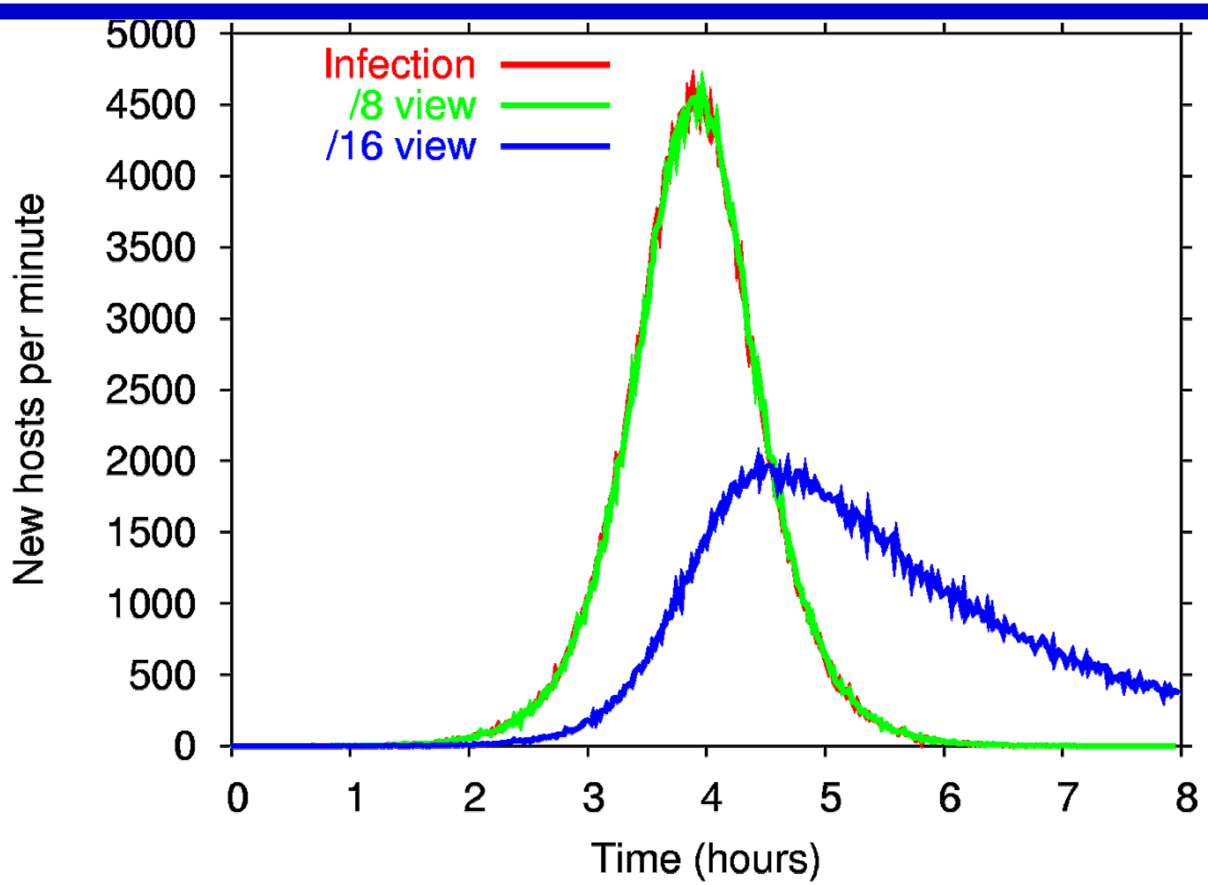
(Code-Red approx. this rate)



- /8 telescope accurately tracks overall behavior of infection
- /16 telescope lags behind in time and shape is misleading

Worm Spread – 10 probes/sec

(Code-Red approx. this rate)



Smaller network telescopes can’t accurately determine event start times (e.g. when a particular host is infected).

Distributed Telescopes

- A distributed telescope uses non-contiguous blocks of address space to increase telescope size.

- Other advantages:
  - Reduces dependency on reachability of single block
  - Traffic load may be spread over multiple sites
  - May avoid being skipped (on purpose or accidentally) by PNRG/address selection algorithms

Distributed Telescopes

- Disadvantages/challenges:
  - Statistics may be trickier – different pieces have different reachability at different times
  - Time synchronization
  - Data distribution

- Some volunteer and commercial efforts already underway

Anycast Telescopes

- Advertise the same address prefix from multiple locations.
- Similar to distributed in advantages and disadvantages to distributed telescopes, except you don't get the diversity of address block ranges.
- May provide shorter (better?) paths for end-hosts to the telescope, which may improve monitoring when the network is overloaded. But monitor coordination might be hard in that situation.

Transit Telescopes

- Traditional telescopes (or IDSes) are near the edge of the network.

- What can we do in the middle of the network?

- Problems/challenges:
  - Each potential source has different set of destination prefixes which can be seen.
  - Visibility changes over time.
  - How do you get statistics right?

Honeyfarms

- What if we don't just passively monitor, but respond to requests?
- Place a massive amount of address space into honeypots.
- Challenges:
  - Do we want 16 million machines (even virtual)?
  - Which traffic should be sent to honeypot? statistical properties, accurate determination of what is happening
  - Just having an IP address isn't enough: email worms go to email accounts, p2p worms go to p2p nodes.
  - Generates more traffic.

Where does that leave us?

- Network telescopes provide insight into non-local network events
- Larger telescopes better capture the behavior of events and can see smaller events
- How do we actually build larger, distributed telescopes and honeyfarms?