
# The Internet's Architecture is Under Attack (Ironically)

**Andrew Sullivan**

IAB Plenary at IETF97, November 2016

Seoul, South Korea

INTERNET
PERFORMANCE.
DELIVERED.

dyn.com @dyn

# Some attacks

- Attacks against Dyn DNS infrastructure
- Noted because of dependent systems
  - AKA “customers”
- I did no direct work on this
- Our NOC and ops did — as NOCs and ops do everywhere — great work under hard conditions
- Leads me to revisit some questions about Internet architecture

# Significant infrastructure

- Anycast-based DNS system
  - Mostly transit rather than peering based
  - At least two transit providers in all sites
  - Transit carefully arranged among sites for resilience
  - Transit diversity to avoid peering-based failures
- Large global installation in 18 sites

# What happened initially?

- Started at 2016-10-21 about 11:10 UTC
  - Like a normal DDoS
- Abrupt change focussed on “US-East” region
  - Many more addresses than usual
  - Not the usual pattern
- Caused some resolution failures, long latency
- Lasted until about 13:20 UTC

# What happened next?

- Started at 2016-10-21 about 15:50 UTC
  - Same as previous attack, only global
- We'd learned from previous attack, and so were able to blunt it some
- Still widely observable
- Second recovery by about 17:00 UTC
- Some resolvers apparently affected until 20:30 UTC
  - Not little, obscure ones

# What was unusual?

- Not the usual amplification attack
  - Very high proportion of TCP
- Not a lot of spoofing
  - 40k addresses confirmed involved, may be up to 100k
- Legit recovery retransmissions functioned as amplifiers
- Mirai-based botnet confirmed
- Apparent “hangover” effect with some resolvers

# Not a one-off

- krebsonsecurity.com was taken down in September by a botnet
- The Mirai botnet source code is now available
  - Like any publicly-available code, it is being improved upon
- I bet you all have your favourite DDoS example

# So, Internet of Things is bad, right?

- Mirai botnet, so lots of “Internet of Things” blame
- There *was* an IoT dimension to this attack
- That’s not the main story
- The attack pattern uses the very thing that makes the Internet strong to attack the Internet architecture

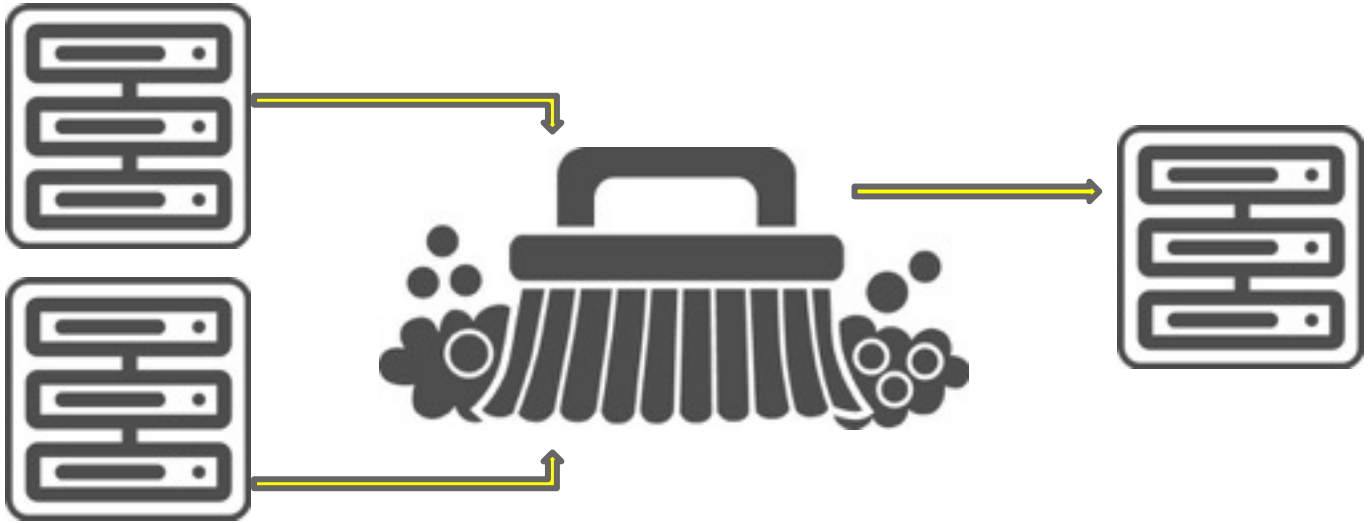
# A simpler time...

Buy from provider

Just check CAIDA to verify spoofing allowed

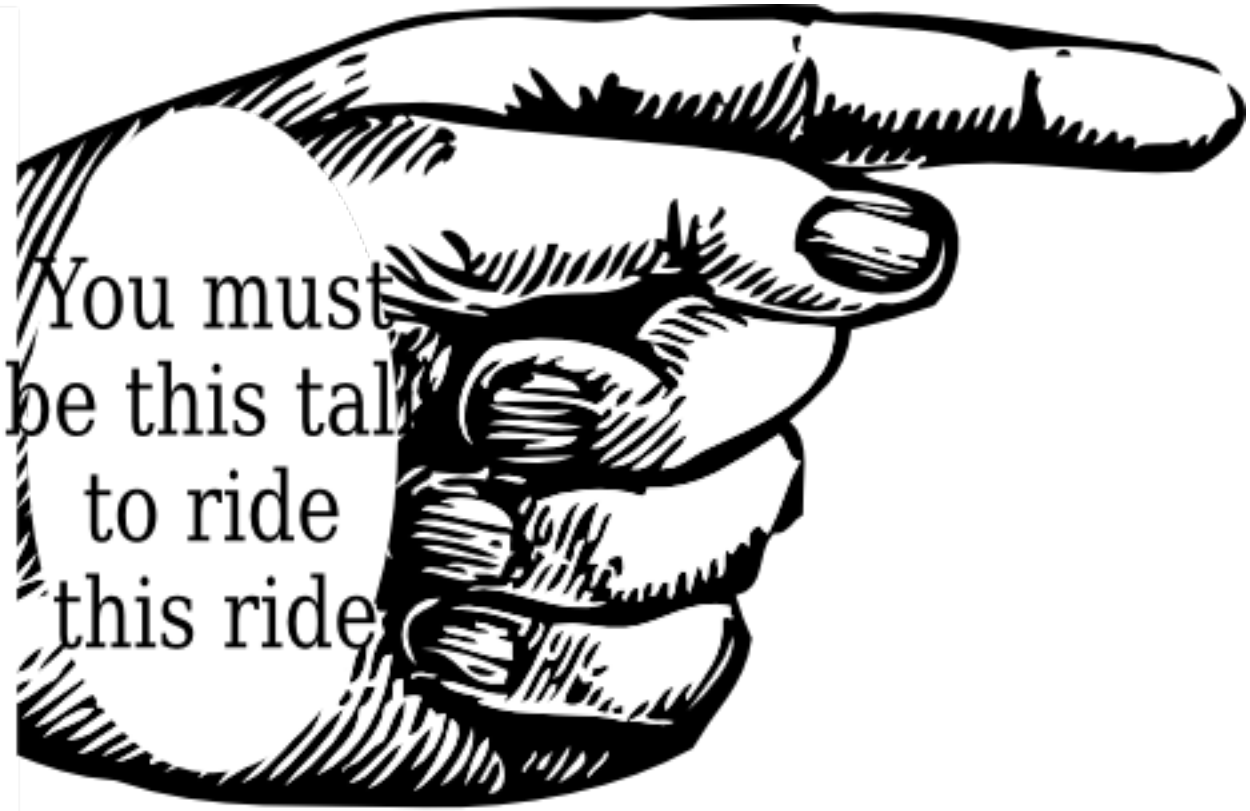
A connected server ( $85 - $150 ) used to orchestrate volume based denial of service attacks (NTP, SSDP, DNS, TFTP, Valve, TeamSpeak… etc)
The focus is on exploiting fundamental Internet protocols: scan the Internet to find reflectors or buy a reflector list ( $25 - $50 )

# Vendors / transit providers improve scrubbing tech

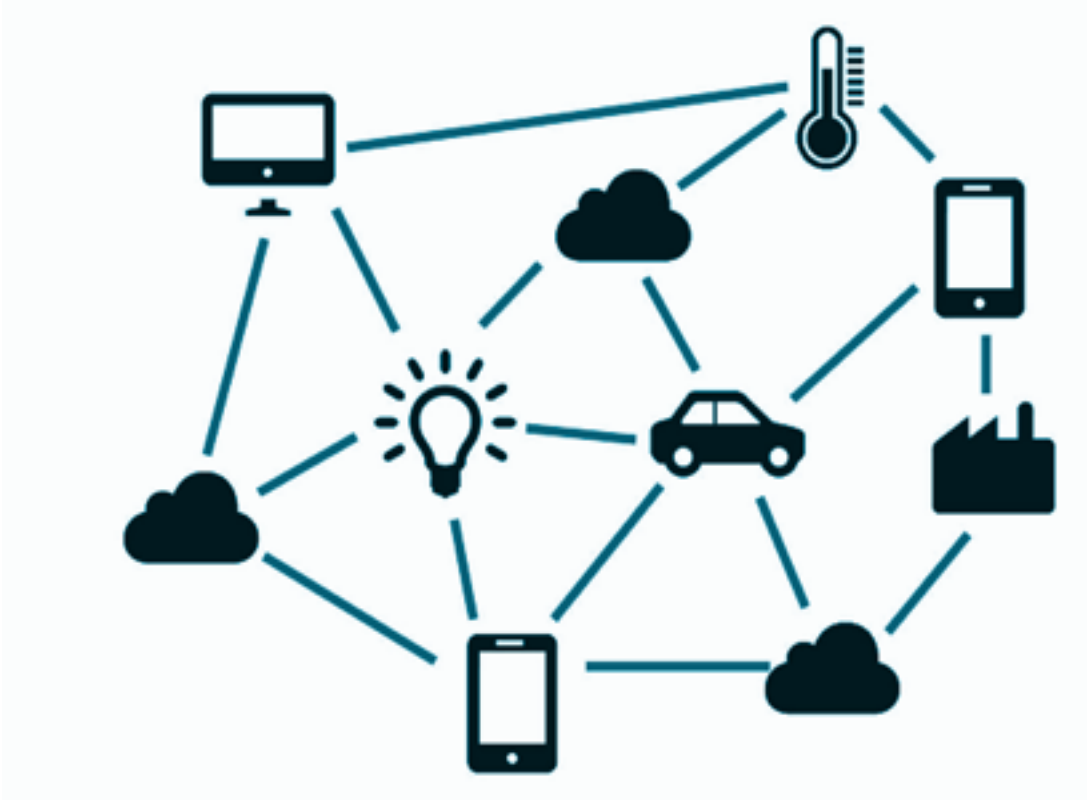


Service providers increase connectivity to soak up and scrub attacks

"Average bandwidth to cause downtime was only 4.3 GB/s" - Security Compass
(Numbers make us all feel more comfortable!)


You must
be this tall
to ride
this ride

# More connected things == more problems?



# Vulnerabilities: fish in a barrel

Fingerprinted a sample of 3,000 IPs (of ~4.1 million unique A record IPs in dynamic dns data).

- 10% of the devices in the sample are affected
- Use case that encourages owners to open them to the Internet.

Example: $vendor's IP Cameras

# Wait. Wasn't this what we *wanted*?

Use case that encourages owners to *open them to the Internet.*

# Remember that dumb network?

- Maximal intelligence at edge
  - Could still be a dumb device
- We want the network to avoid making a lot of decisions
  - Easier to upgrade endpoints
  - People who want the advantages have the incentive to upgrade

# This is what makes for the attack

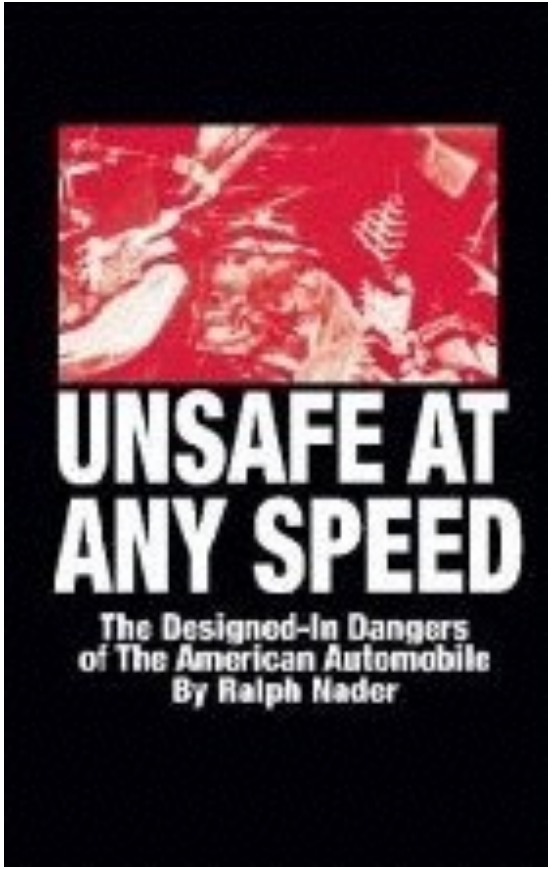
- *Really bad* story when too many of the endpoints are bad guys
- IoT is just a means to this end
- Insecurity of devices is not the main problem
- None of this is DNS- or even UDP-specific
- Limited improvement from more providers
  - Which also create more barriers to entry

# Proposals I have personally heard

- Government-mandated BCP 38 implementation
  - Doesn’t always help
- License to connect
  - Devices or people
- Top-speakers preferred access for DNS
  - Submission for DNS?
- Your end-of-open-network answer here

The roots of the unsafe vehicle problem are so entrenched that the situation can be improved only by the forging of new instruments of citizen action.

—Ralph Nader in the Preface



# Are there things we could do?

Build on the tradition of the network of networks

- Why can’t network devices or applications advertise what kinds of traffic they want to send?
- Why can’t network devices or applications advertise what scope they want to be in?
  - HOMENET is in the right ballpark, but not yet proposing this?
- New feedback mechanisms?  Manufacturer Usage Description?
- Would anything we do be an invitation to better or new attacks?

# DISCUSS

# Image credits

- Slide 9: Shady character image. Source https://pixabay.com/en/hacker-www-binary-internet-code-1446193/. ©2014, bykst. Used under CC0 license.
- Slide 11: Must be this tall. Source http://www.clker.com/clipart-you-must-be-this-tall.html. ©2010, Chris on clker.com. Used under CC0 license.
- Slide 17: Dust cover of *Unsafe at Any Speed*. Source https://en.wikipedia.org/wiki/File:Unsafeatanyspeedcover.jpg. Used under fair use. ©unknown
- Slide 19: Chevrolet Corvair. Source https://commons.wikimedia.org/wiki/File:Chevrolet_Corvair_(2995960853).jpg?uselang=en-ca ©2007, dave_7. Used under Creative Commons Attribution 2.0 Generic