ORACLE + Dyn

The Internet of Infrastructure Threats

IoT, DDoS, and Future Internet Architecture

Andrew Sullivan

NIST IoT Cybersecurity Colloquium

Thanks to my colleagues Chris Baker and Marshall Everson

Who Am I & Why Should You Believe Me?

- Working on Internet Infrastructure since 2001
  - Especially DNS
- At Oracle Dyn since 2012
- Internet Architecture Board from 2013 to 2017
  - Chair from 2015-2017
- Primary concern: resilience and scalability of Internet

My views are not necessarily those of the Oracle Corporation.

The Internet's Distributed Architecture

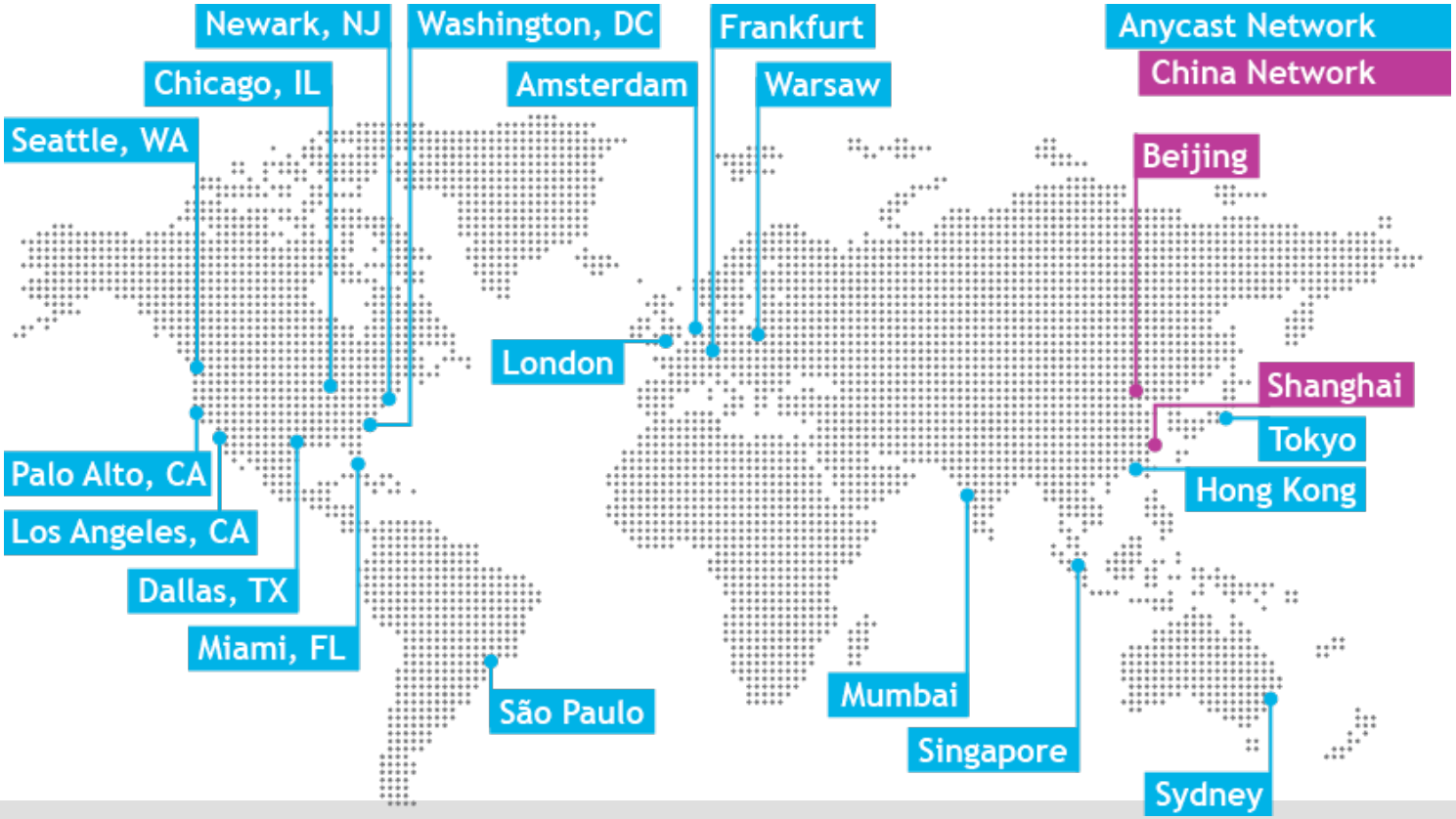
IDEAL

- Mostly distributed
- Resilience through operational diversity
- Mostly small operations for specific purposes
- Many, many operators

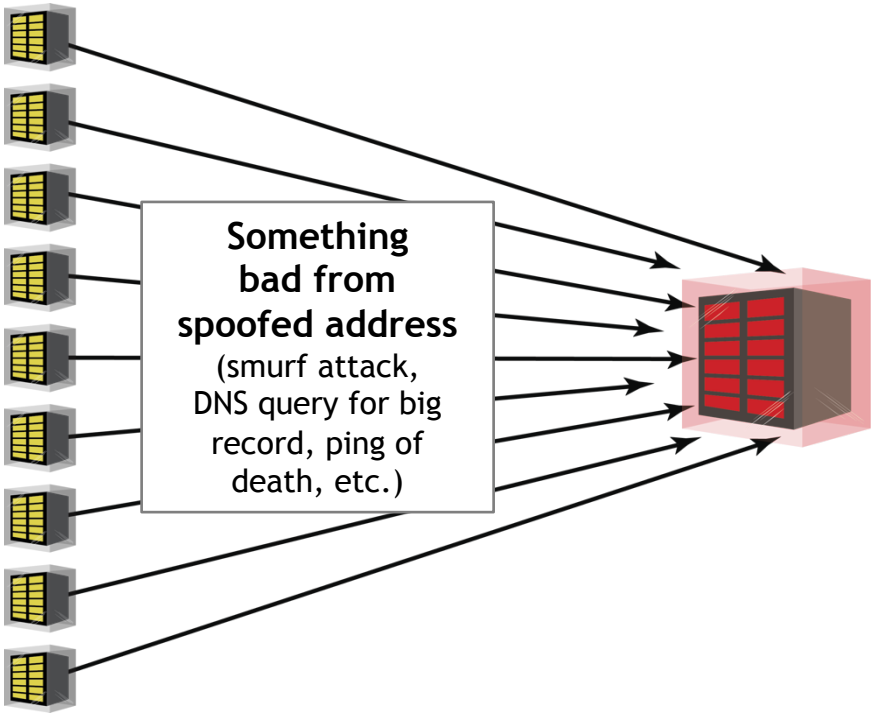
ACTUAL

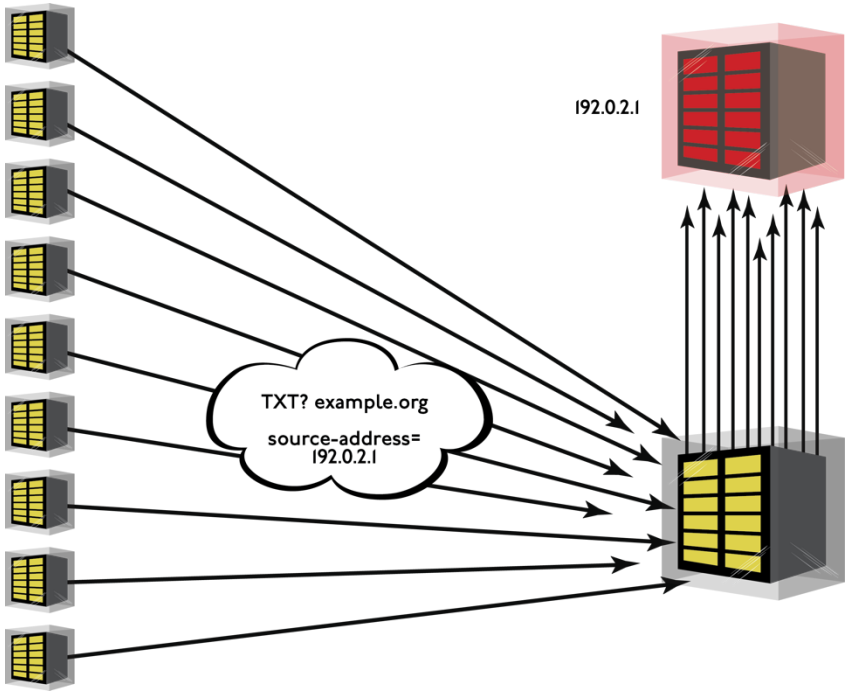
- Highly concentrated
- Resilience through operational scale
- Distributed operations by a few large players & common protocols
- A few huge operators, and a long tail of tiny ones

An Example: Oracle Dyn Anycast Network

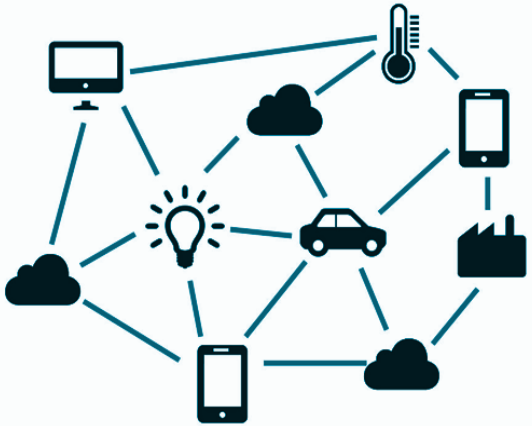


Reminder: DDoS Has Flavours





IoT: A New Botnet Environment!



Reminder: Bots and Botnets

- **Bot**: An autonomous program on a network (especially the Internet) that can interact with computer systems or users.
- **Botnet**: A network of private computers infected with (usually) malicious software and controlled as a group (usually) without the owners' knowledge.
- **Bot herder**: An individual who controls and maintains a botnet by installing botnet software in numerous machines, putting these machines into his or her control.

Why?

- Espionage
- Chaos
  - Includes cyber-war, terrorism, &c.
- Money

“Keep Up With Patches” Not Enough

We will run out of time before They run out of compromises

- 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: IP Cameras
  - Use case of many devices promotes bandwidth and computing power

This is what we wanted!

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

All About Incentives

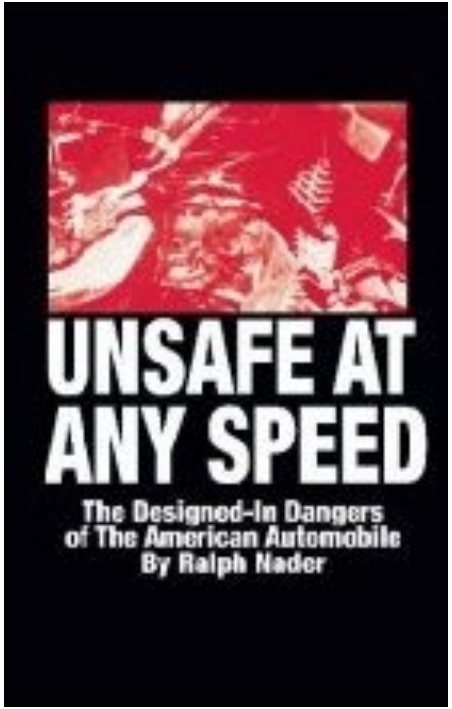
1. Incentives for security are backwards: Usability is harder
2. Pressure to ship == ship soon, secure later
3. More devices than people

End-to-end Need Not Mean Network Endpoint

- End-to-end model is often interpreted to mean “network endpoint”
- Better understood as end of functional communication
  - Need not be at endmost point
  - Application perspective needed
- We forgot that many networks are nevertheless “Internet sites”
  - No network manager != not a network
- Create the incentives for safe operation
  - S.1691 a good move in this way

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



Some Will Be Keen To See Outright Regulation

Treaties Take Time

Time we don’t have

What Is To Be Done?

- Continue to pursue incentives for vendors
- Build (your) infrastructure with multiple providers
- Promote and develop good tools for unmanaged networks
  - Internet Engineering Task Force HOMENET, &c.
- Understand control points
  - Building everything with controls back in the cloud means service failure if you can't reach the cloud
  - The Internet's design is more resilient, so buy systems that work that way

ORACLE + Dyn

Thank you!