Knowledge of Internet Structure: Measurement, Epistemology, and Technology

David Clark

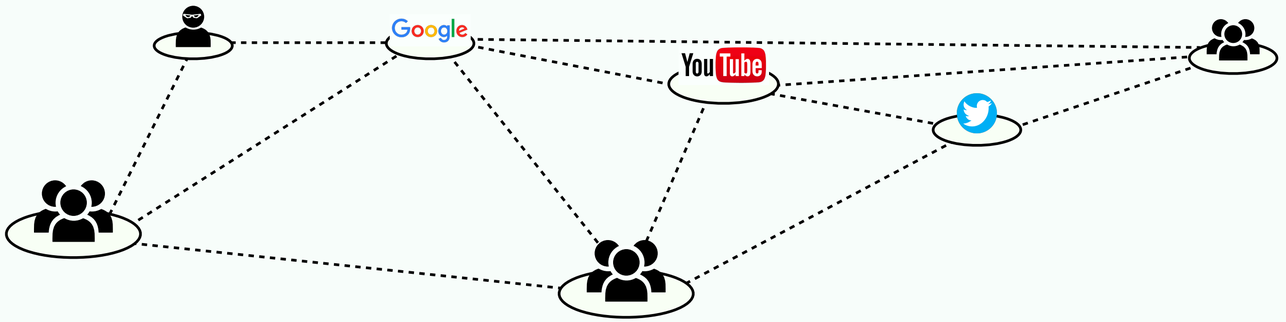
kc claffy

C-Accel Team A-7165

Why are we home during this pandemic?

The Internet is
holding society together
(and *saving lives*)

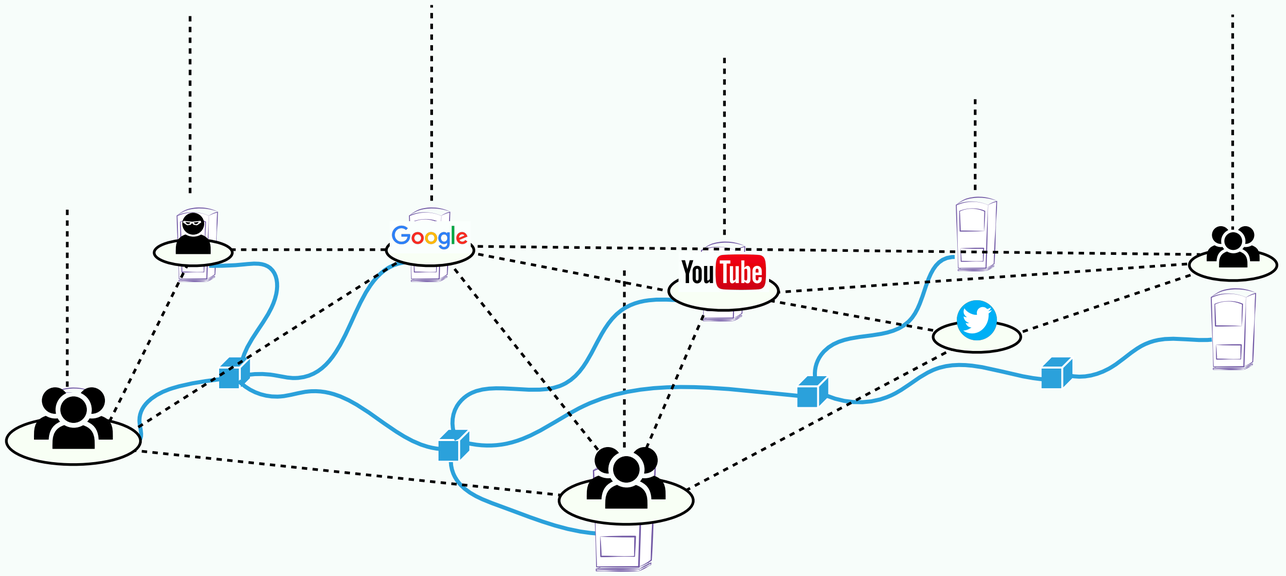
Because we
can be.



What holds the Internet together?

Plumbing we rarely hear about,
highly vulnerable to
misconfiguration and abuse.

What's under
the hood?

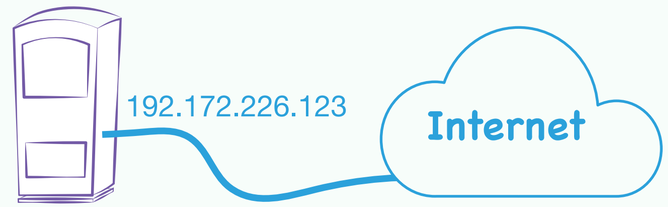


three key Internet systems

Domain Naming System

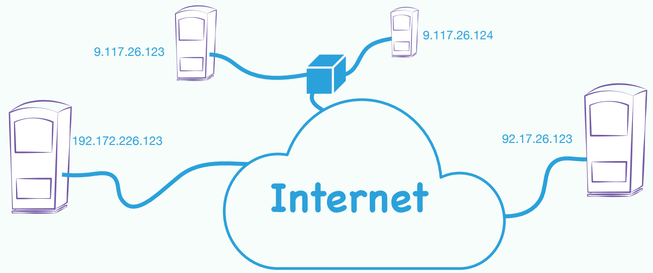
maps names to **addresses**
(www.caida.org)

Addressing Architecture



provides **addresses for connected devices**
(12.3.4.5)

Interdomain Routing System

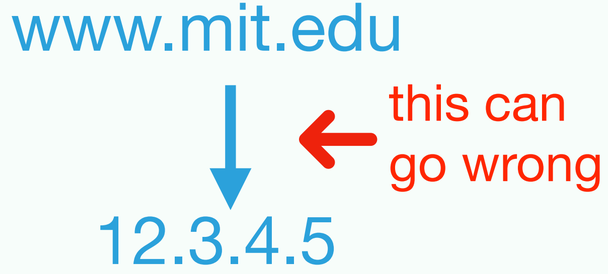


determines **paths to those addresses**
(12.3.4.0/24)

trusting plumbing

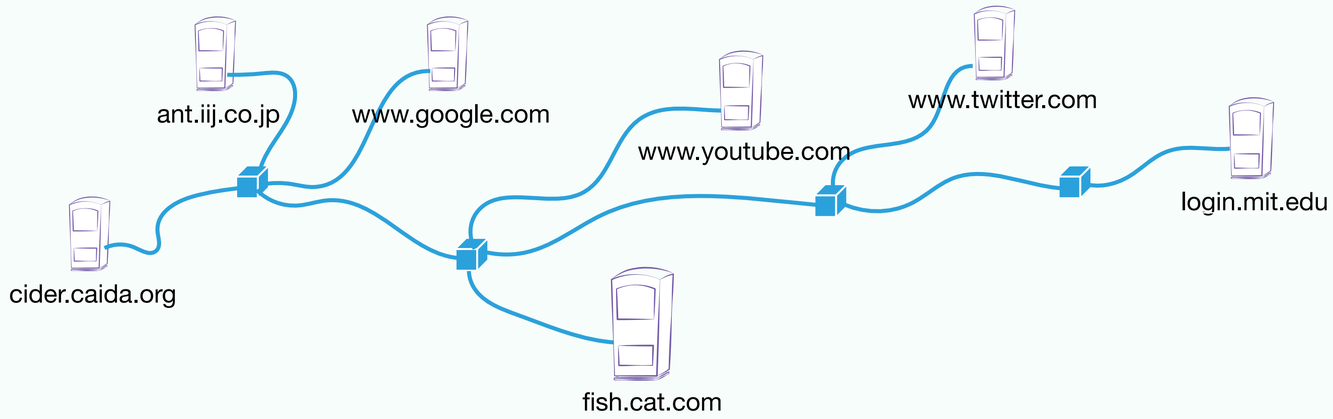
Naming

maps **domain names**
(www.mit.edu)
to **addresses**



- 740K domain names associated with abuse
- *proprietary data/inferences*

— ICANN monthly DAAR report April 2020



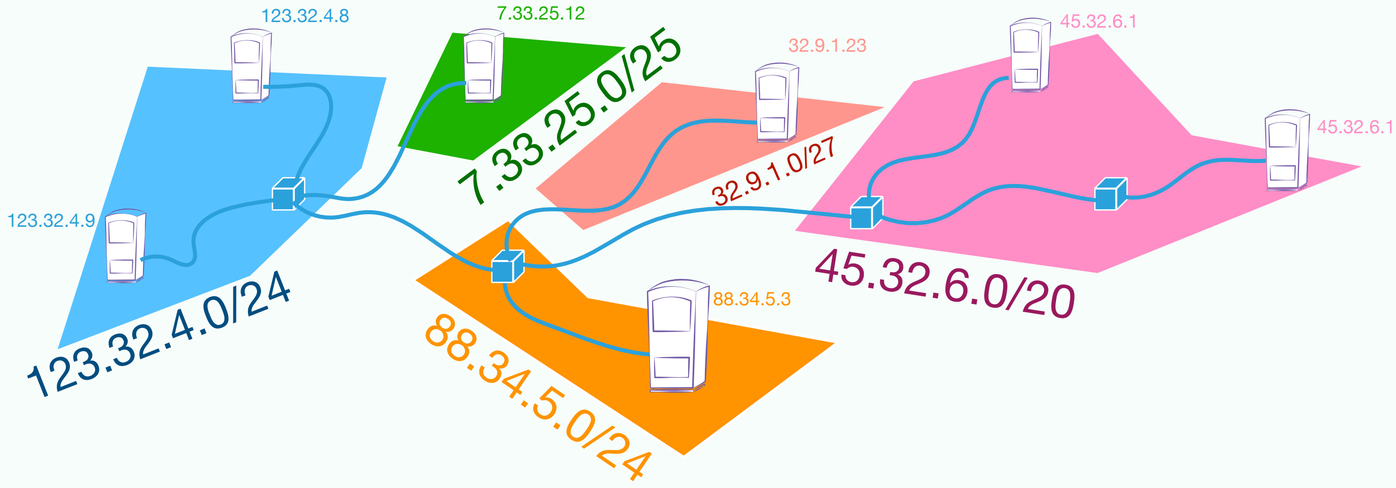
trusting plumbing

Naming

provides **addresses** for connected devices (12.3.4.5)

Addressing

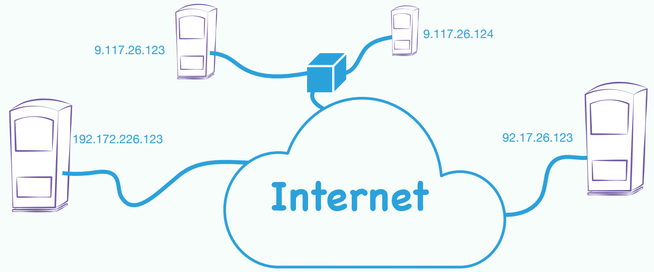
- spoofing to launch attacks, evade policies, impersonate



trusting plumbing

Naming

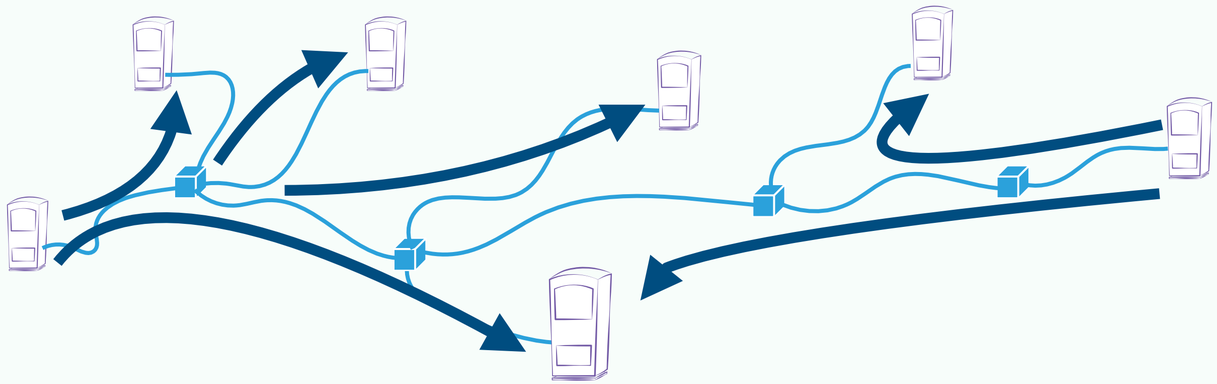
determines **paths** to those addresses (12.3.4.5)



Addressing

- abuse of routing to steal cryptocurrency
- …or generate $29M fraudulent ad revenue

Routing



why problems persist for decades

historically

- academic roots of Internet architecture
- did not assume adversaries in devices
- once threat model was clear…

approaches have been

- technical, neglecting political economy
- global in scope, or no benefit
- complex, expensive, *architectural* changes…

incompatible with reality

- lowest cost operational practices
- some governments less focused on security
- all governments lack *knowledge*

team leadership

kc claffy

caida

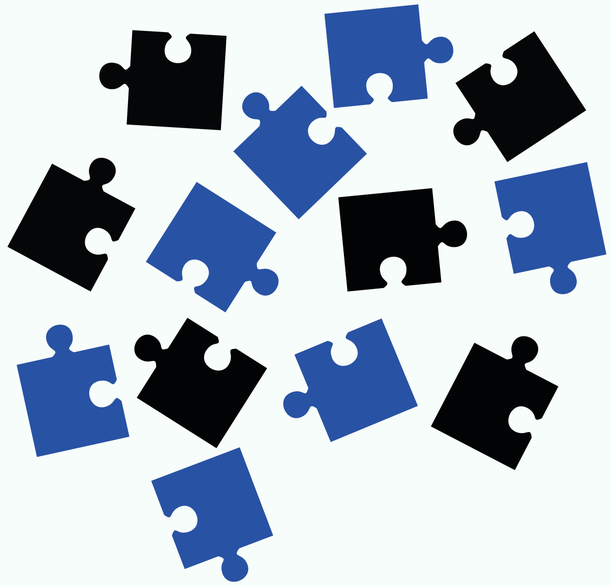
- Director, Center for Applied Internet Data Analysis
- Research Scientist and Adjunct CSE faculty, UCSD
- 30 years of experience with Internet data analysis

David Clark

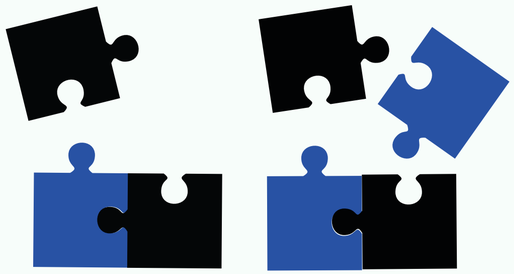
CSAIL

- Development of Internet protocols since 1970s
- Chaired Internet Architecture Board 1981-1989
- Tech.Dir. of MIT Internet Policy Research Institute
- Recent book ``Designing an Internet" (NSF program)

the problem

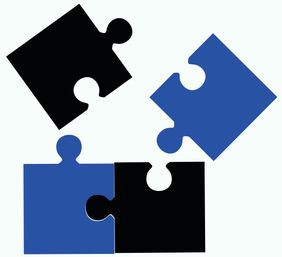


data-rich (sort of)

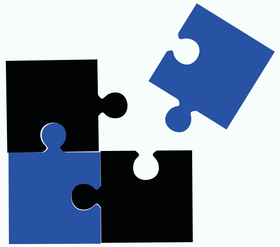


knowledge-poor

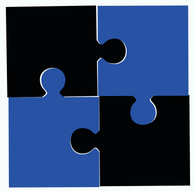
the solution



1) Increase open knowledge



2) Inform operational practices



3) Enforce operational practices

operational practices: routing

“code of conduct”

1) *Prevent illegitimate routes*
2) *Correct contact info in DBs*
3) *Publish routing policies*
4) *Prevent forged traffic*

MANRS

Mutually Agreed Norms for Routing Security

But are ISPs complying?

[Internet Society]

When compliance measured..

Participating networks are not complying any more than others.

Network Hygiene, Incentives, and Regulation: Deployment of Source Address Validation in the Internet", ACM Computer and Comm. Security (CCS), Nov 2019.

MANRS

Mutually Agreed Norms for Routing Security

Driving Insight

OKN needed

Phase I confirmed that open knowledge network is required to demonstrate compliance with routing security best practice.

2-year roadmap

Year 1: Technical knowledge

- Identify properties consistent w/misbehavior
- Tools to understand & remediate configuration problems
- Catalog best practices (BGP, DNS)
- Begin to translate into actionable knowledge

Year 2: Actionable knowledge

- Cross-disciplinary cross-sector cross-jurisdictional
- Align incentives
- Extend, socialize, accelerate deployment of practices
- Sustainability

A-7165 OKN: KISMET

academic


David Clark


kc claffy

Massachusetts Institute of Technology

CSAIL

caida

UC San Diego
JACOBS SCHOOL OF ENGINEERING
Computer Science and Engineering

UNIVERSITY OF OREGON

BRIGHAM YOUNG UNIVERSITY
FOUNDED 1875
BYU
PROVO, UTAH

government

NIST
National Institute of Standards and Technology

ESnet
ENERGY SCIENCES NETWORK

industry

Interisle Consulting Group

VERISIGN

FARSIGHT SECURITY

COMCAST

pir

non-profit

DNS-OARC

Internet Society

M3AAWG

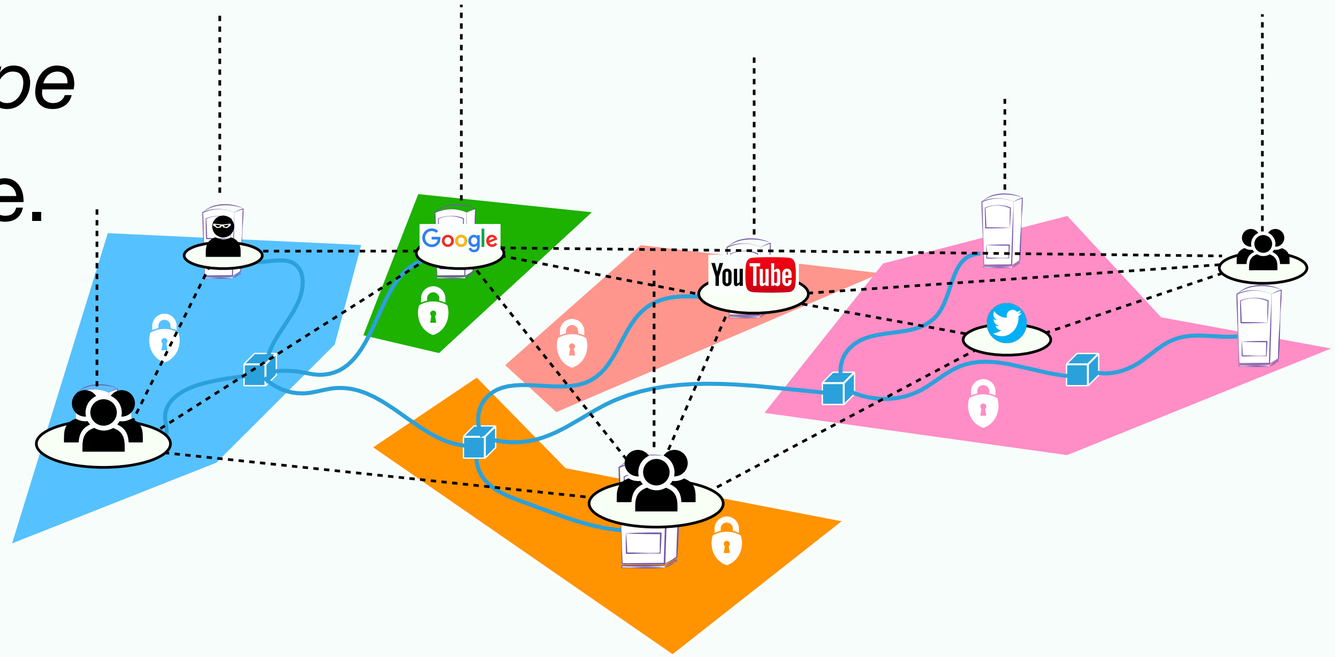
SDN LABS

project summary

We propose a knowledge network to improve the security and functioning of three key but inherently vulnerable systems that underpin all activity on the Internet, including all OKNs!

Change security landscape
from reactive to proactive.

Treat the Internet like the critical infrastructure it is.



A-7165 Booth Agenda

Presentation at 0:15 and 0:45 after the hour!

Please type questions into Q&A popup window.

https://www.caida.org/projects/kismet/