DNS Privacy, Service Management, and Research: friends or foes?

John Heidemann
USC/ISI

ISOC DNS Privacy Workshop
San Diego, 2016-02-26

Copyright © 2017 by John Heidemann
Release terms: CC-BY-NC 4.0 international
Different Challenges

DNS privacy

DNS service management

DNS research
Different Stakeholders

- DNS users
- DNS privacy
- computer
- DNS research
- researchers
- DNS service management
- operators

DNS Privacy Thoughts / 2017-02-26
Different Problems

DNS privacy

operators

need to run DNS:
why 10k q/hour from 192.0.2.1?
...oh, they’re for johnsiphone.usc.edu

researchers

need to learn things:
my new IDS found 10k q/hour?
was it an attack?
or a bug in my IDS?

DNS can leak information:
johnsiphone.usc.edu A?
goingggle.com A?

computer

users

DNS service management

DNS can leak information:
johnsiphone.usc.edu A?
goingggle.com A?
(My Perspective)

DNS privacy

(I do some of each of these things)

DNS service management

researchers

computer users

operators
Traditionally: Users Aren’t Concerned

DNS Privacy

DNS can leak information: johnsiphone.usc.edu A ? googggle.com A ?

computer

users

here google, keep my grocery list
...doubleclick.net: apples now on sale at cornershop.com

here comcast, take me to googggle.com
...let me redirect your NXDOMAIN to my search page to monetize that

researchers

operators

DNS service management DNS research
Traditionally: Operators Keep the Lights On

need to run DNS:
why 10k q/hour from 192.0.2.1?
...oh, they’re for johnsiphone.usc.edu

10k q/hour from 192.0.2.1
...hmm, what does tcpdump tell us

how can we fix this?
...oh, that data is from rm 1141,
maybe they were hacked
Traditionally: Researchers Make Do

my new IDS found 10k q/hour? ...hmm, does ground truth help verify that?

or perhaps today ...no access to ground truth, my algorithm must be perfect, time to publish!

DNS research

need to learn things:
my new IDS found 10k q/hour: was it an attack? or a bug in my IDS?
What Do We Want?

- Users deserve privacy (without asking)
- Operators need to find and fix problems
- Researchers need research to be possible

DNS privacy

Computer users

DNS service management

Operators
Trends

• new **technical methods** improve DNS privacy
  – DNS over TLS: anti-eavesdropping
  – qname minimisation: share less with auth. servers
  – both are standardized, but deployment is early

• new **policies** to manage disclosure
  – helps where technical means are not enough
Trends

• **new technical methods** improve DNS privacy
  – DNS over TLS: anti-eavesdropping
  – qname minimisation: share less with auth. servers
  – *both are standardized, but deployment is early*

• **new policies** to manage disclosure
  – helps where technical means are not enough
Trends

• new technical methods improve DNS privacy
  – DNS over TLS: anti-eavesdropping
  – qname minimisation: share less with auth. servers
  – both are standardized, but deployment is early

• new policies to manage disclosure
  – helps where technical means are not enough
Suggestions for Operators

• will shift to in-server-software logging
  – not just passive packet capture

• perhaps anonymized logging by default
  – keep data at rest “safe”
  – perhaps reversible for debugging,
    but only on demand, with auditable logs
Suggestions for Researchers

• researchers need data
  – some may be sensitive
  – an *old* problem (consider medical research)

• perhaps formalize research access to data
  – an explicit process, not back-room handshake
  – can constrain what is shared
    • minimize the contents
    • review needs (Institutional Research Boards)?
    • agree (by policy) data will not be joined to de-anon.
  – further drill-down will be needed, but hopefully rarely
Context: the Broader DNS “Ecosystem”

• for operations
  – US laws: CALEA, ECPA, Stored Comm. Act, etc.
  – also international laws, like in EU
  – need to consider how these are handled inside orgs

• for researchers
  – Menlo Report—how principles from medical ethics apply to computer research
  – some academic conferences now require an “ethics statement” in papers
Where From Here?

• challenge
  – can we flip the switch to “default private”?
  – with a “narrow on” with auditing, for operations and research?

• questions
  – for researchers, would this be better than today?
  – for operators, could you still do your job?
  – for users (and user watchdogs), better? sufficient?