DNS Privacy

dnsprivacy.org

Sara Dickinson
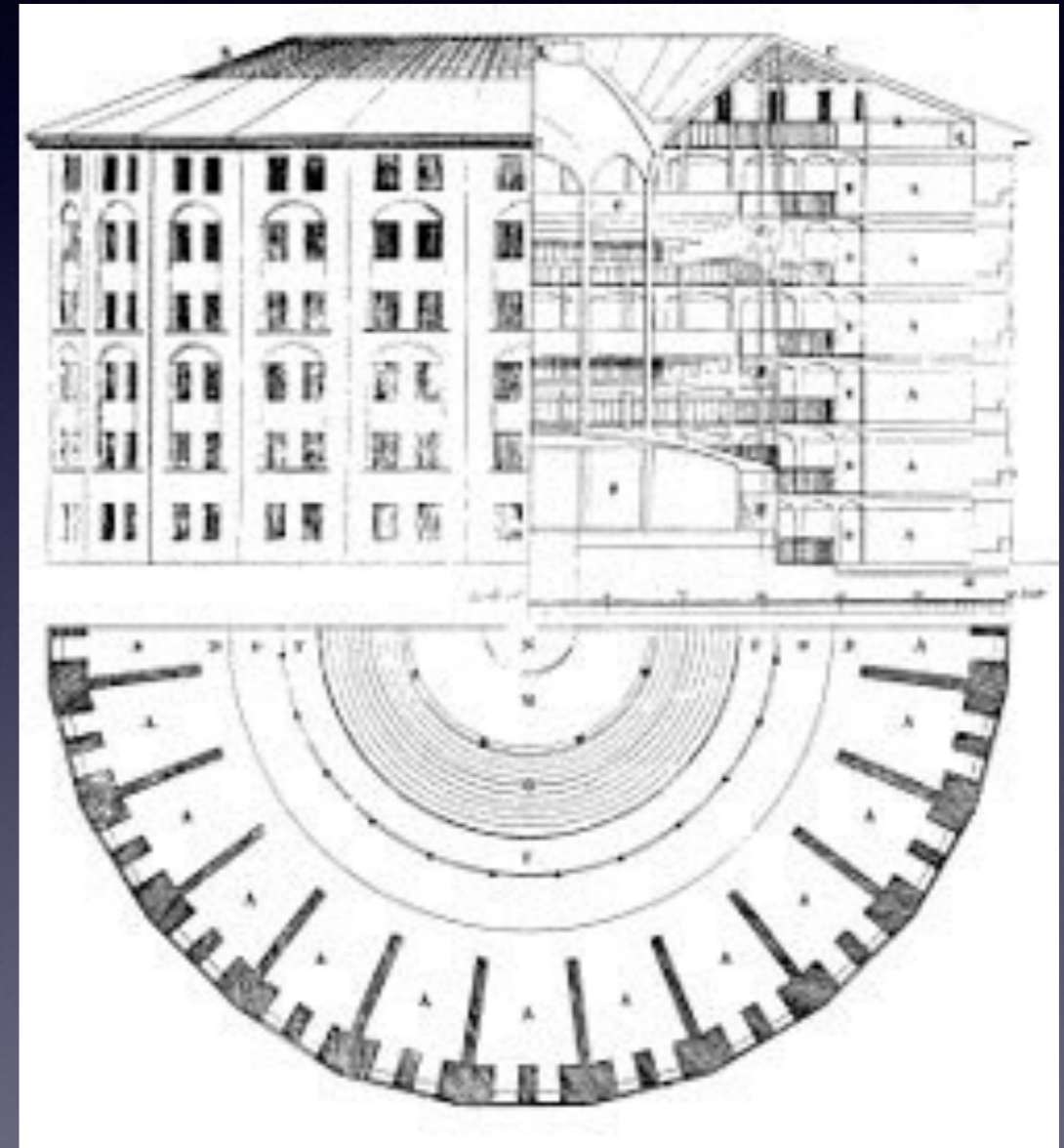Sinodun (Salesforce, NLnet Foundation)
sara@sinodun.com

Overview

- **The problem:** Why Internet privacy and DNS Privacy are important (DNS leakage)

- **Recent Progress:** Chart progress during last 3-4 years (DPRIVE)

- **Where are we now?** Present current status and tools
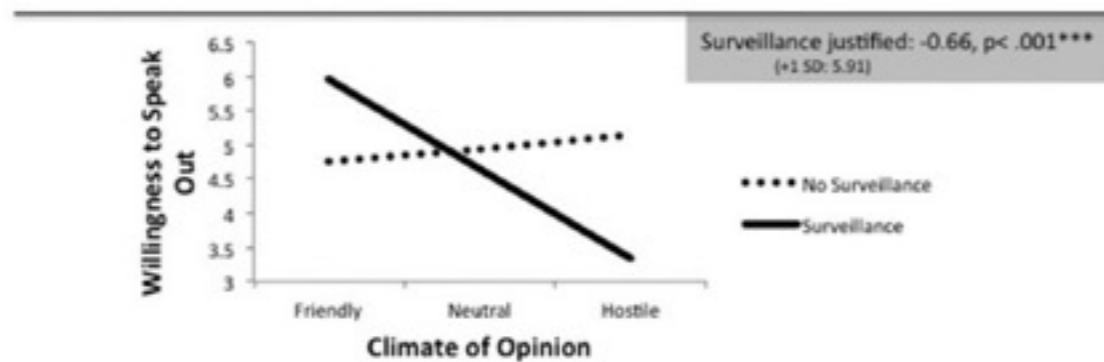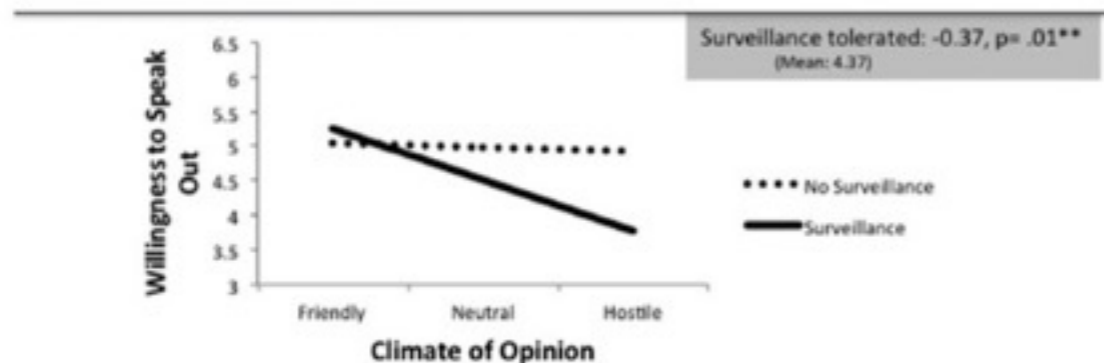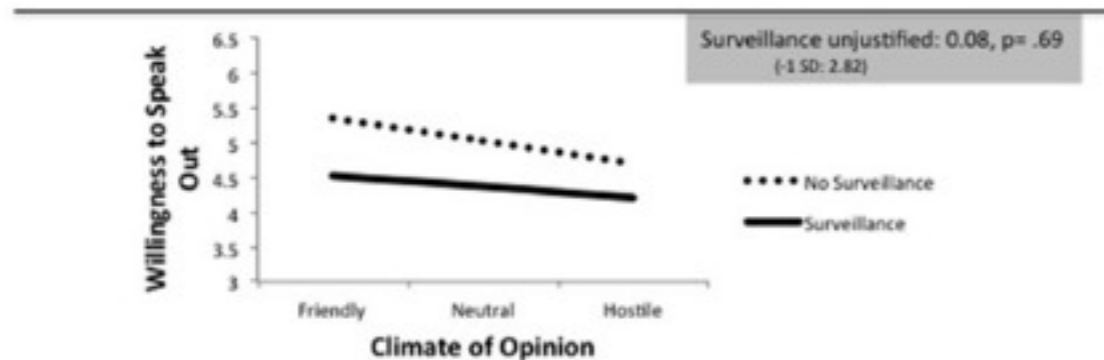
Internet Privacy

Slides from: Daniel Kahn Gillmor (ACLU)

Why does internet privacy matter?

- Surveillance as social control

- Machine learning at scale today means small number of people controlling network can perform mass surveillance

Behaviour changes
(even when no-one is watching)

Surveillance unjustified: 0.08, p= .69
(-1 SD: 2.82)

Surveillance tolerated: -0.37, p= .01**
(Mean: 4.37)

Surveillance justified: -0.66, p< .001***
(+1 SD: 5.91)

Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring

Elizabeth Stoycheff, Journalism & Mass Communication Quarterly 1-16

DNS is part of the leaky boat problem

DNS

Traffic size

TLS SNI

....?

Timing patterns
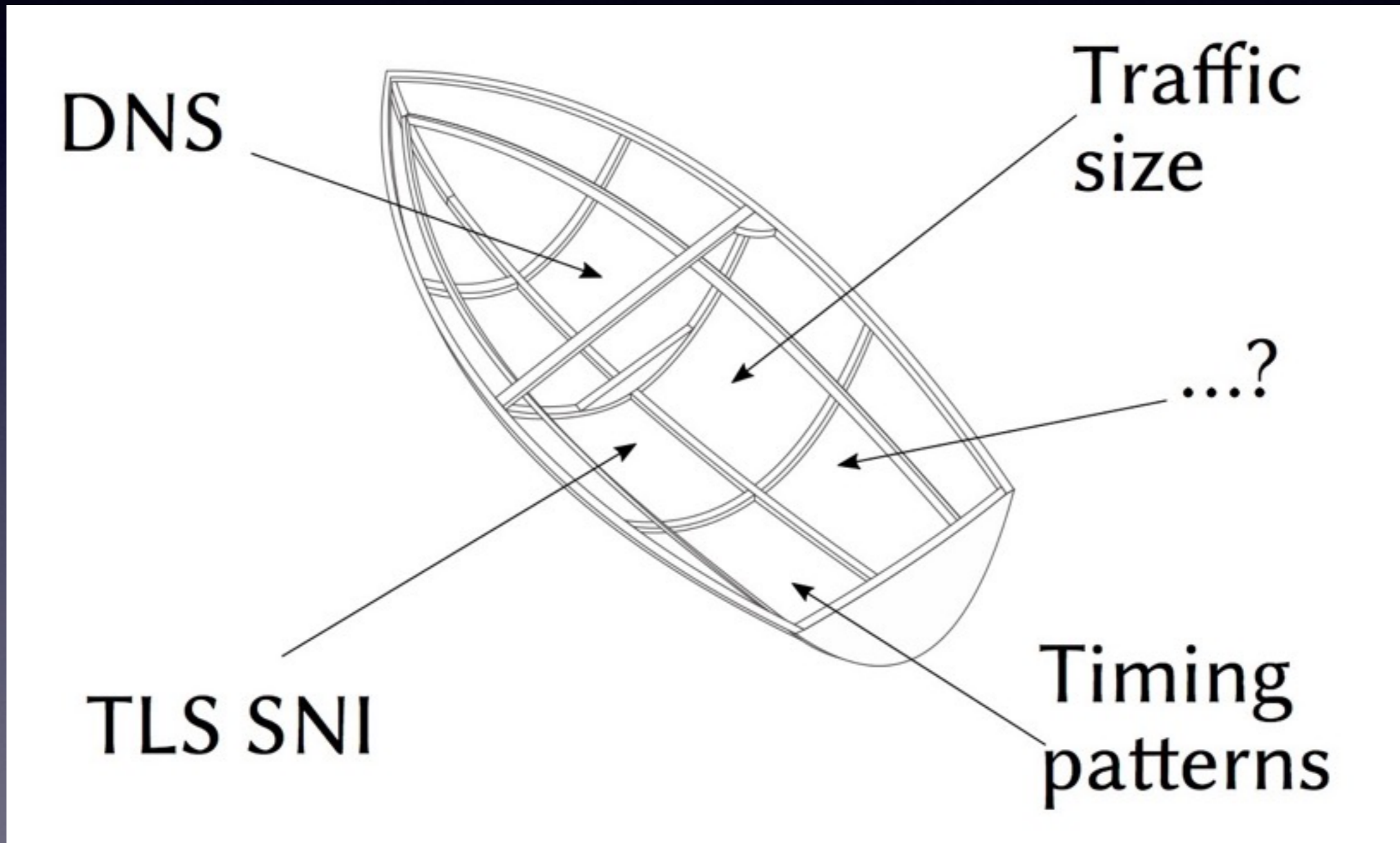
DNS Privacy
- A brief history

IETF Privacy activity

March 2011	**I-D:** Privacy Considerations for Internet Protocols (IAB)
June 2013	Snowdon revelations What timing!
July 2013	**RFC6973:** Privacy Considerations for Internet Protocols
May 2014	**RFC7258**: Pervasive Monitoring is an Attack: "**PM is an attack on the privacy of Internet users and organisations**."

RFC 7258

"**PM is an attack on the privacy of Internet users and organisations**."

"…that needs to be **mitigated** where possible, **via the design of protocols** that make PM significantly more expensive or infeasible**. "
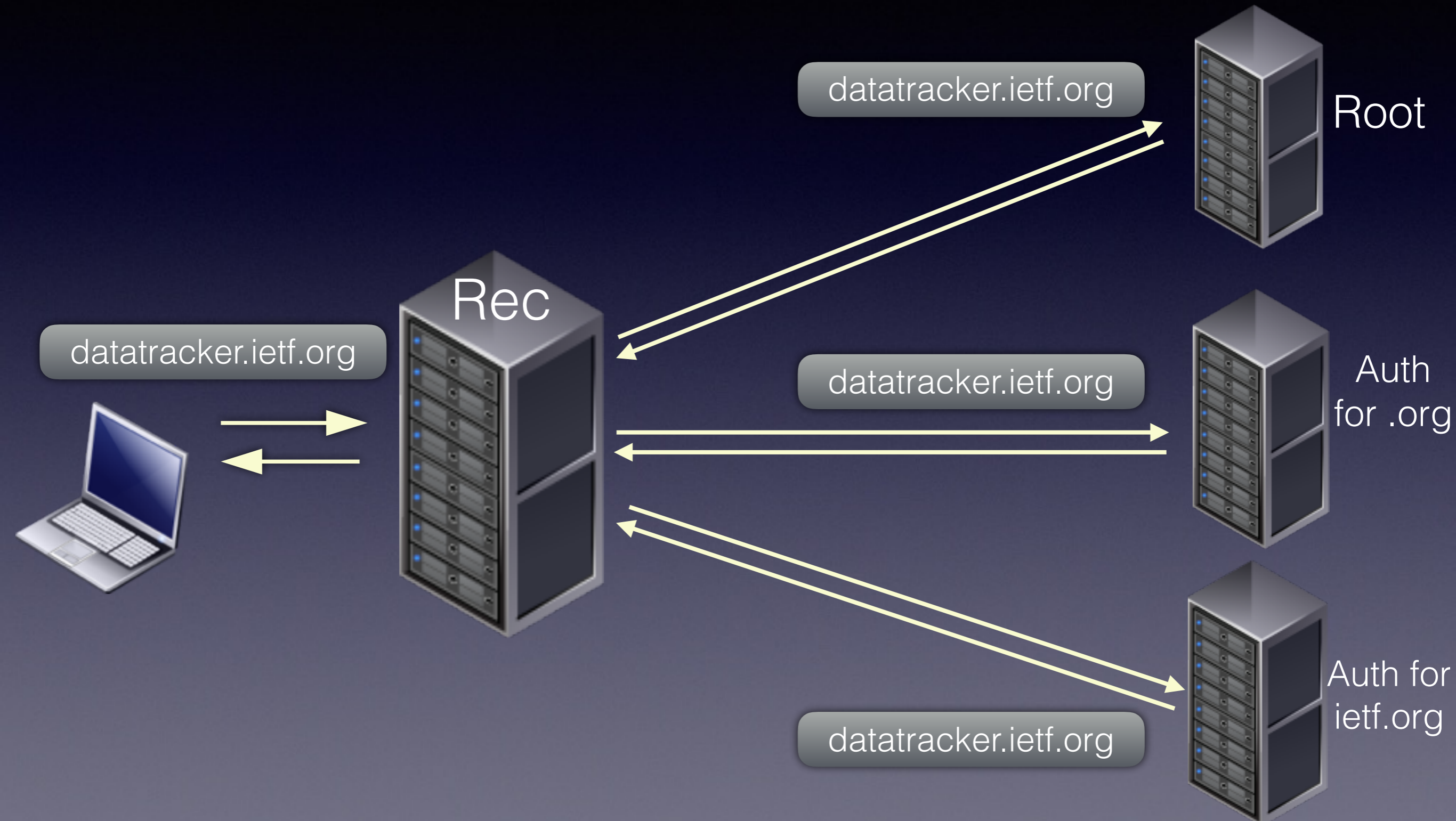
DNS Privacy in 2013?
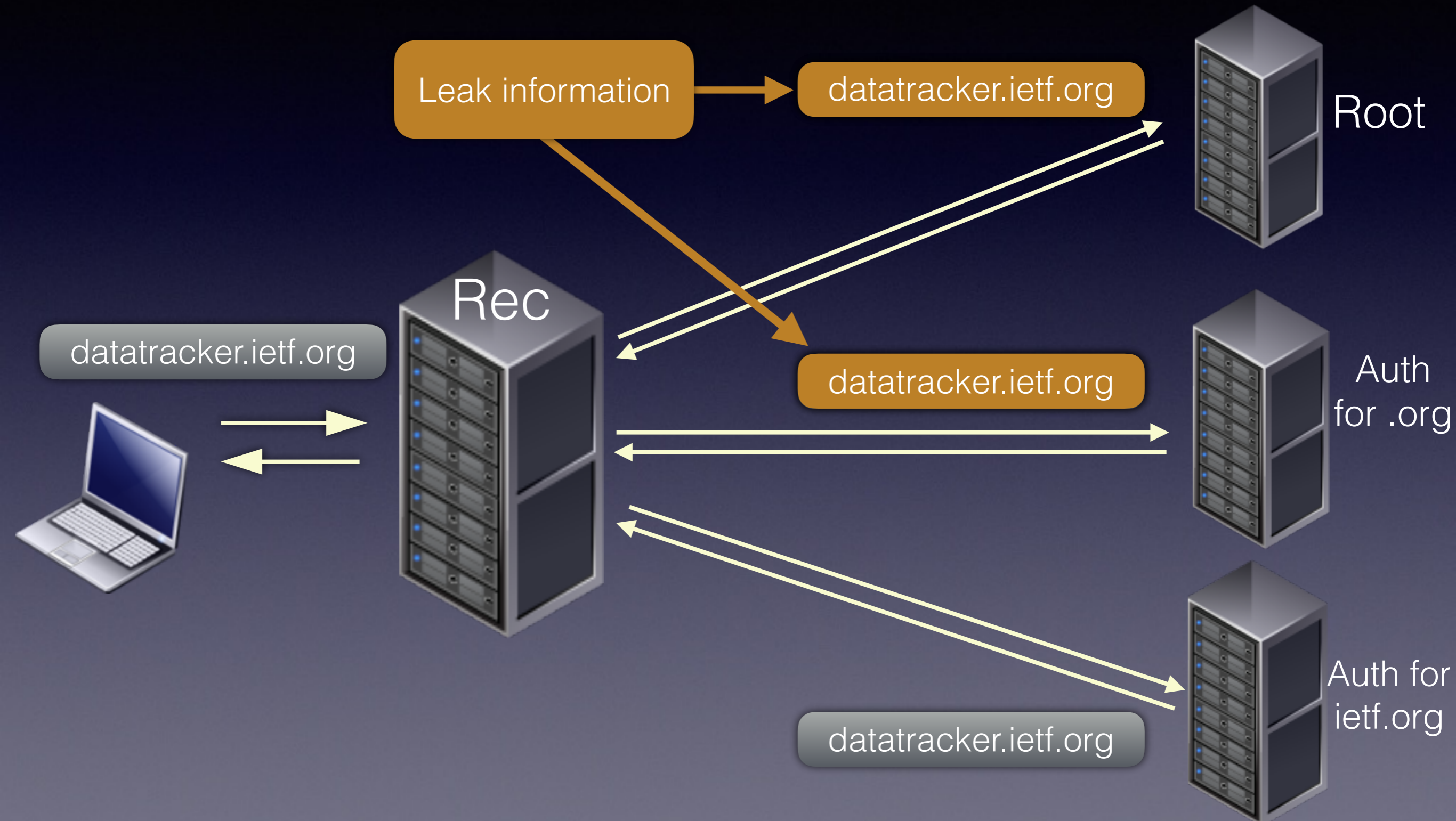

- DNS is 30 year old! [RFC1034/5 (1987)]

  - Original design availability, redundancy and speed!

  - DNS is an 'enabler'

- DNS standards:

  - UDP (99% of traffic to root)

  - TCP only for 'fallback' (pre 2010)

> DNS sent in clear text
> -> NSA: '**MORECOWBELL**'

- Perception: The DNS is public, right? It is not sensitive/personal information….it doesn't need to be protected/encrypted

DNS Disclosure Example 1

datatracker.ietf.org

Root

datatracker.ietf.org

Rec

datatracker.ietf.org

Auth for .org

Auth for ietf.org

datatracker.ietf.org

DNS Disclosure Example 1

Leak information → datatracker.ietf.org

Root

datatracker.ietf.org

Rec

datatracker.ietf.org

Auth for .org

Auth for ietf.org

datatracker.ietf.org

EDNS0 problem

- **RFC6891**: Extension Mechanisms for DNS (EDNS0)

  Intended to enhance DNS protocol capabilities

- But…. mechanism enabled addition of **end-user data into** DNS queries (non-standard options)

EDNS0 problem

- **RFC6891**: Extension Mechanisms for DNS (EDNS0)

Intended to enhance DNS protocol capabilities

- But…. mechanism enabled addition of **end-user data into** DNS queries (non-standard options)

ISP justification: Parental Filtering (per user)

CDN justification: Faster content (geo location)

DNS Disclosure Example 2

Parental Filtering

ietf.org ?
[00:00:53:00:53:00]

Stub

CPE

Rec

Auth

[User src address]
MAC address or id
in DNS query

DNS Disclosure Example 2

Parental Filtering

CDN Geo-location

ietf.org ?
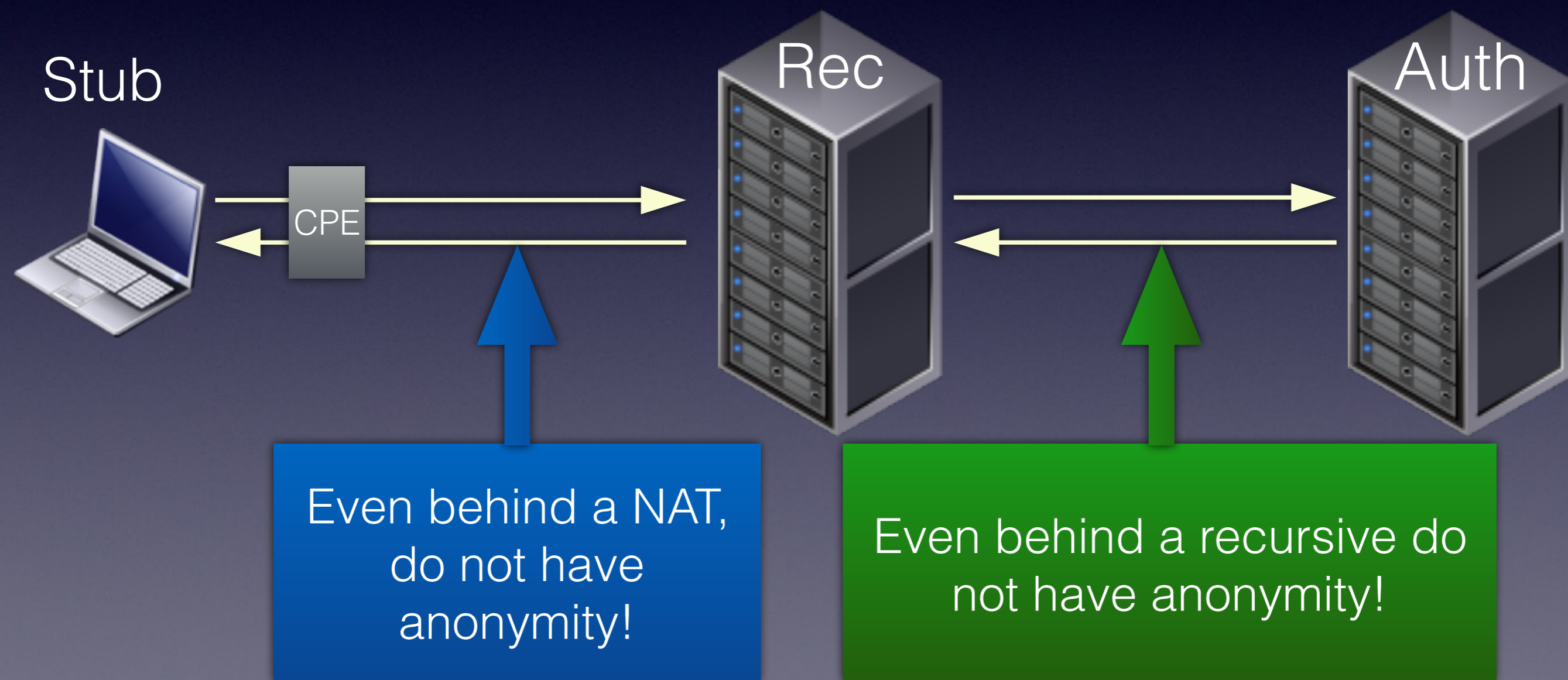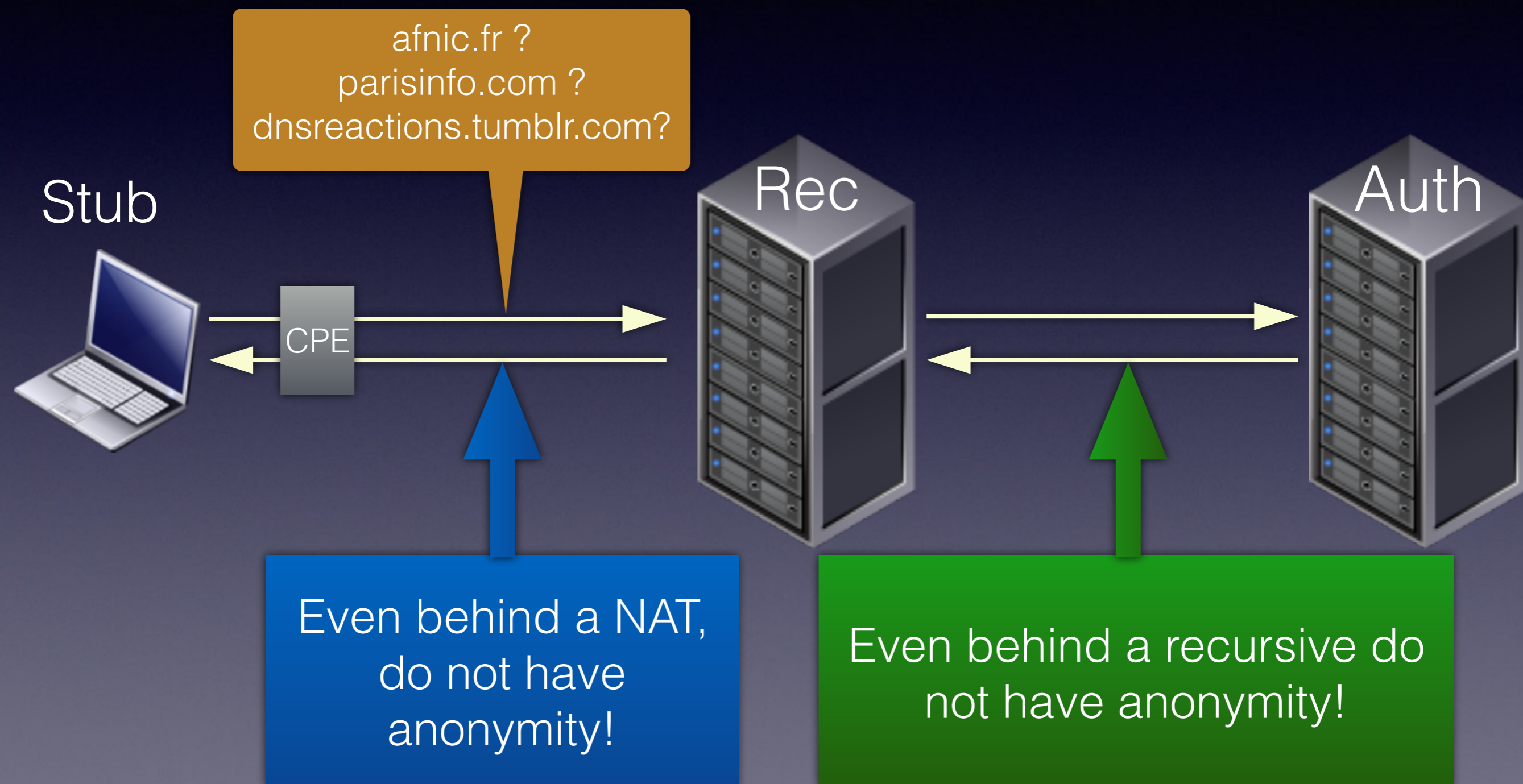[00:00:53:00:53:00]

? ietf.org ?
[192.168.1]

Stub

Rec

Auth

CPE

[User src address]
MAC address or id
in DNS query

Client Subnet (RFC7871)
contains source subnet
in DNS query

DNS Disclosure Example 2
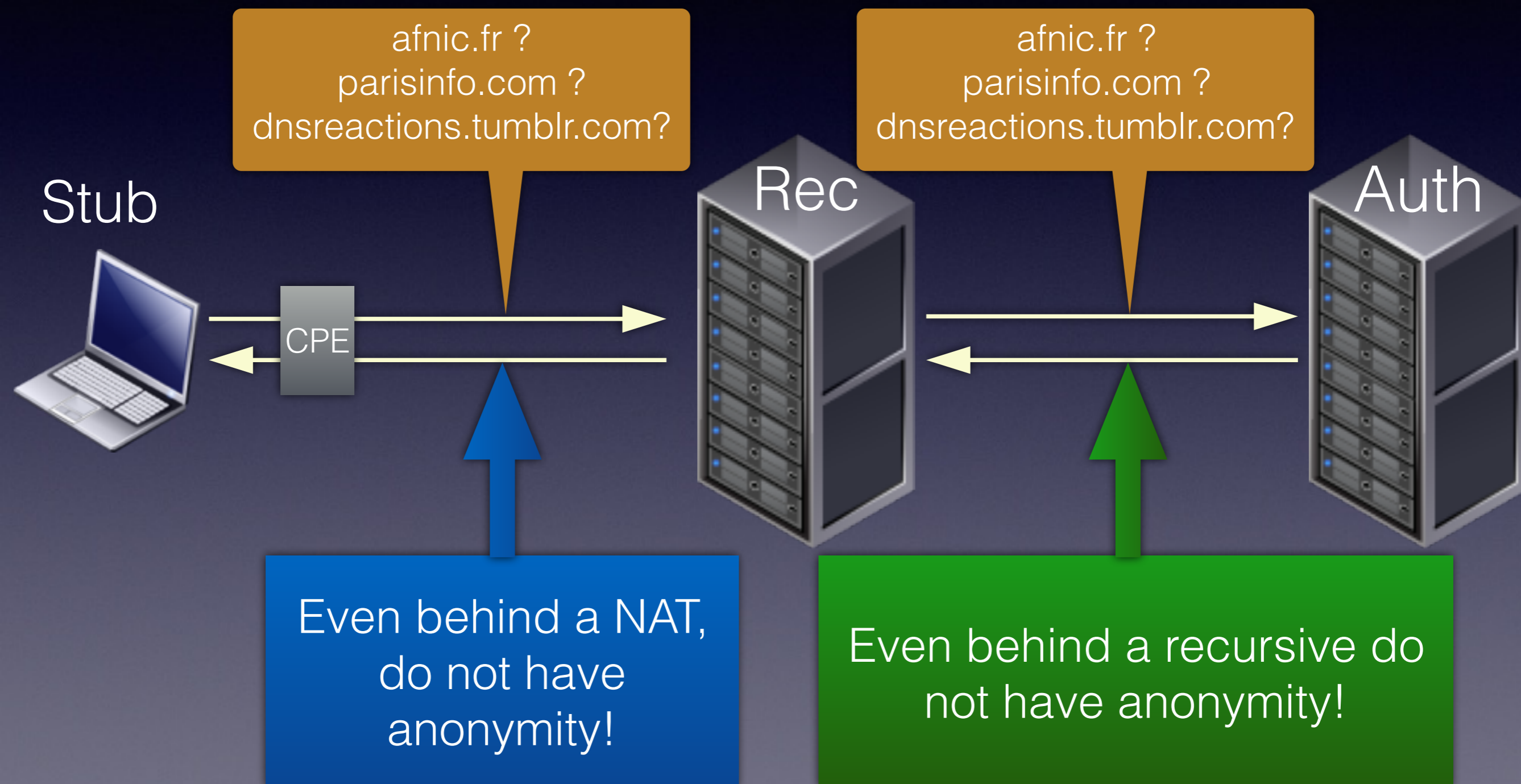
Stub

Rec

Auth

CPE

Even behind a NAT, do not have anonymity!

Even behind a recursive do not have anonymity!

DNS Disclosure Example 2

afnic.fr ?
parisinfo.com ?
dnsreactions.tumblr.com?

Stub

CPE

Rec

Auth

Even behind a NAT, do not have anonymity!

Even behind a recursive do not have anonymity!

DNS Disclosure Example 2

Stub

afnic.fr ?
parisinfo.com ?
dnsreactions.tumblr.com?

CPE

Rec

afnic.fr ?
parisinfo.com ?
dnsreactions.tumblr.com?

Auth

Even behind a NAT, do not have anonymity!

Even behind a recursive do not have anonymity!

DNS: It's not just for names

- MX records (email domain)

- SRV records (services)

- OPENPGPKEY (email addresses)

- …this is only going to increase….

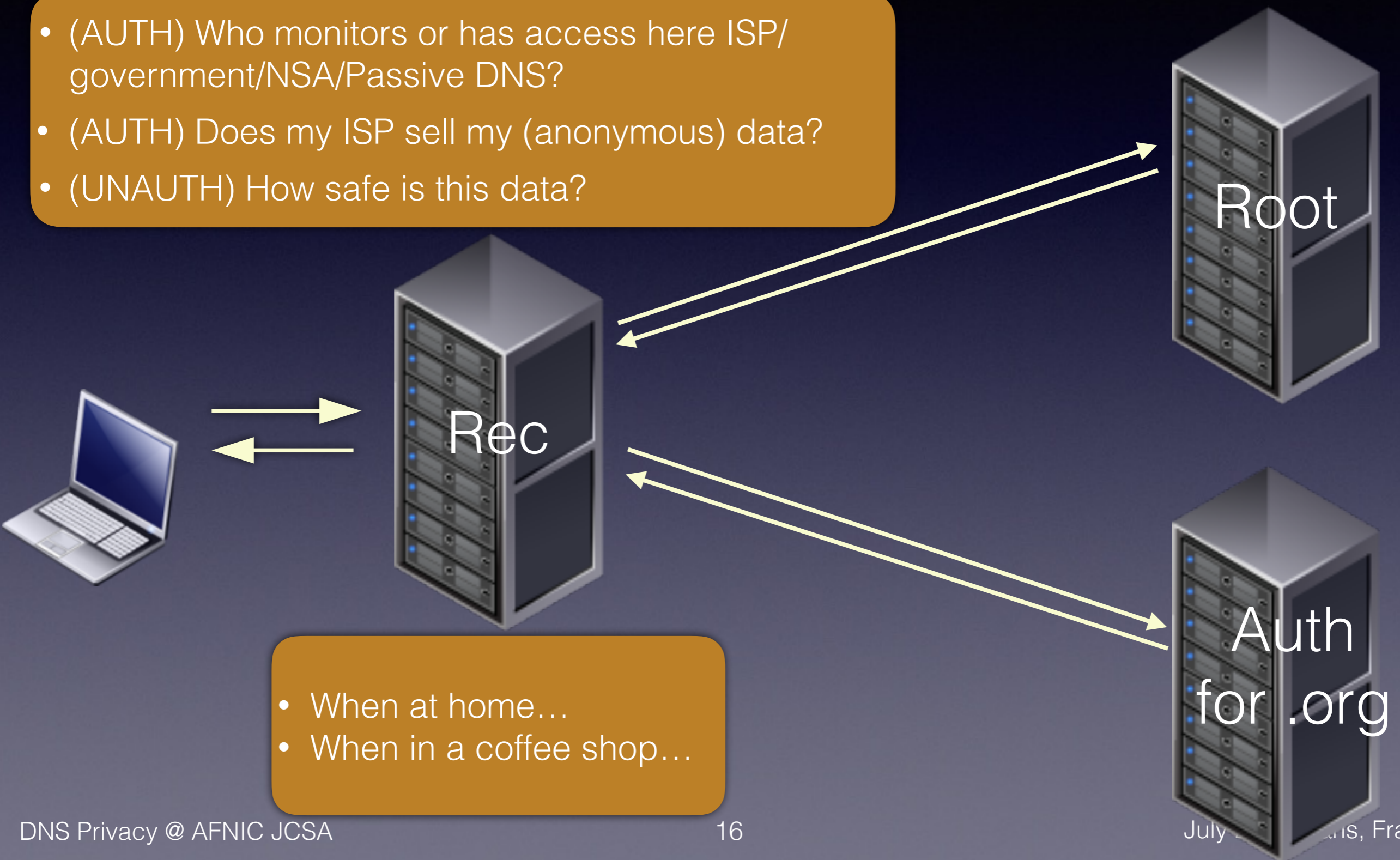# DNS: It's not just for names

- MX records (email domain)

- SRV records (services)

- OPENPGPKEY (email addresses)

- …this is only going to increase….

DNS Disclosure Example 3

- (AUTH) Who monitors or has access here ISP/government/NSA/Passive DNS?
- (AUTH) Does my ISP sell my (anonymous) data?
- (UNAUTH) How safe is this data?

Root

Rec

Auth for .org

- When at home…
- When in a coffee shop…

DNS Disclosure Example 3

- (AUTH) Who monitors or has access here ISP/ government/NSA/Passive DNS?
- (AUTH) Does my ISP sell my (anonymous) data?
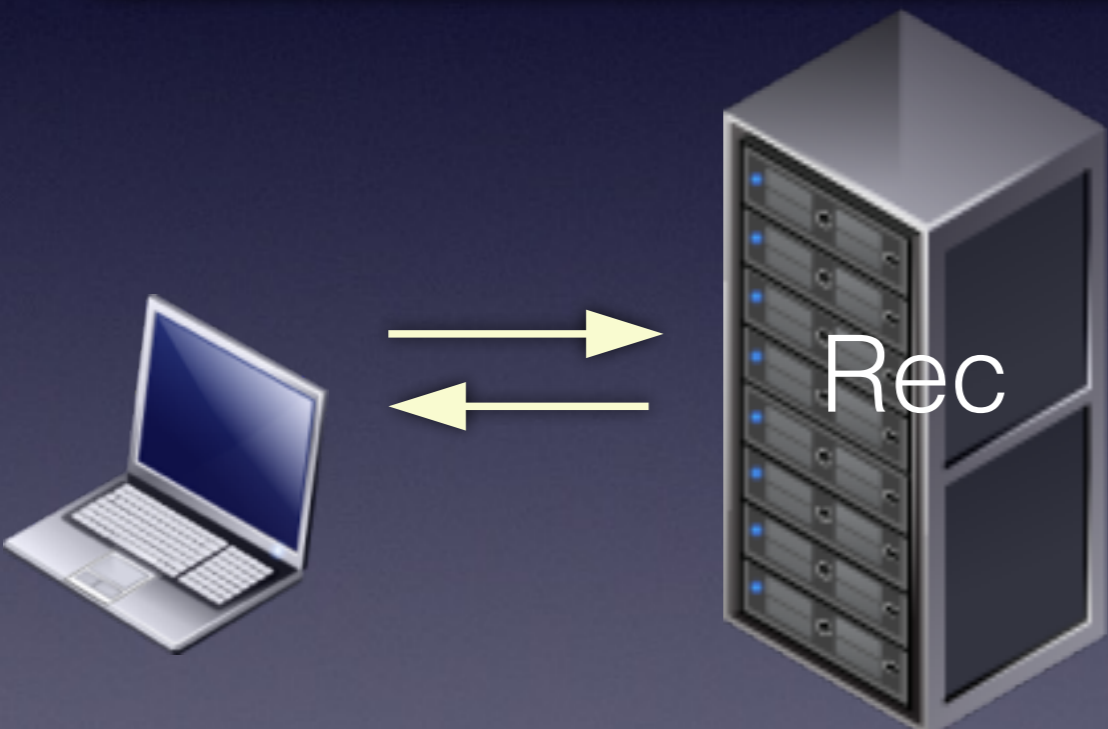- (UNAUTH) How safe is this data?

Who monitors or has access here?

Root

Rec

Auth for .org

- When at home…
- When in a coffee shop…

Who monitors or has access here?

DNS - leakage

- Basic problem is leakage of meta data

  - Allows fingerprinting and re-identification of individuals

- Even without user meta data traffic analysis is possible based just on timings and cache snooping

- Operators see (and log) your DNS queries

DNS - leakage

- Basic problem is leakage of meta data

  - Allows fingerprinting and re-identification of individuals

- Even without user meta data traffic analysis is possible based just on timings and cache snooping

- Operators see (and log) your DNS queries

DNS Risk Matrix

Risk	In-Flight		At Rest	
	Stub => Rec	**Rec => Auth**	**At Recursive**	**At Authoritative**
Passive Monitoring	●	●		
Active Monitoring	●	●		
Other Disclosure Risks e.g. Data breaches			●	●

DPRIVE WG
et al.

DPRIVE WG

- <u>DPRIVE WG</u> create in 2014

> <u>Charter</u>: Primary Focus is
> Stub to recursive

- **Why not tackle whole problem?**

  - Don't boil the ocean, stepwise solution

  - Stub to Rec reveals most information

  - Rec to Auth is a particularly hard problem

WE SHOULDN'T BE EXPLORING OTHER PLANETS UNTIL WE'VE SOLVED ALL OUR PROBLEMS HERE ON EARTH.

SOUNDS REASONABLE. SO, WHAT'S THE TIMELINE ON "SOLVING ALL PROBLEMS"?

TEN YEARS? FIFTEEN?

DNS Privacy problem

Relationship:
1 to 'a few'
some of whom
are know (ISP)

Rec

Root

Relationship:**1 to many** most
of whom are not known
=> Authentication is hard

Auth
for .org
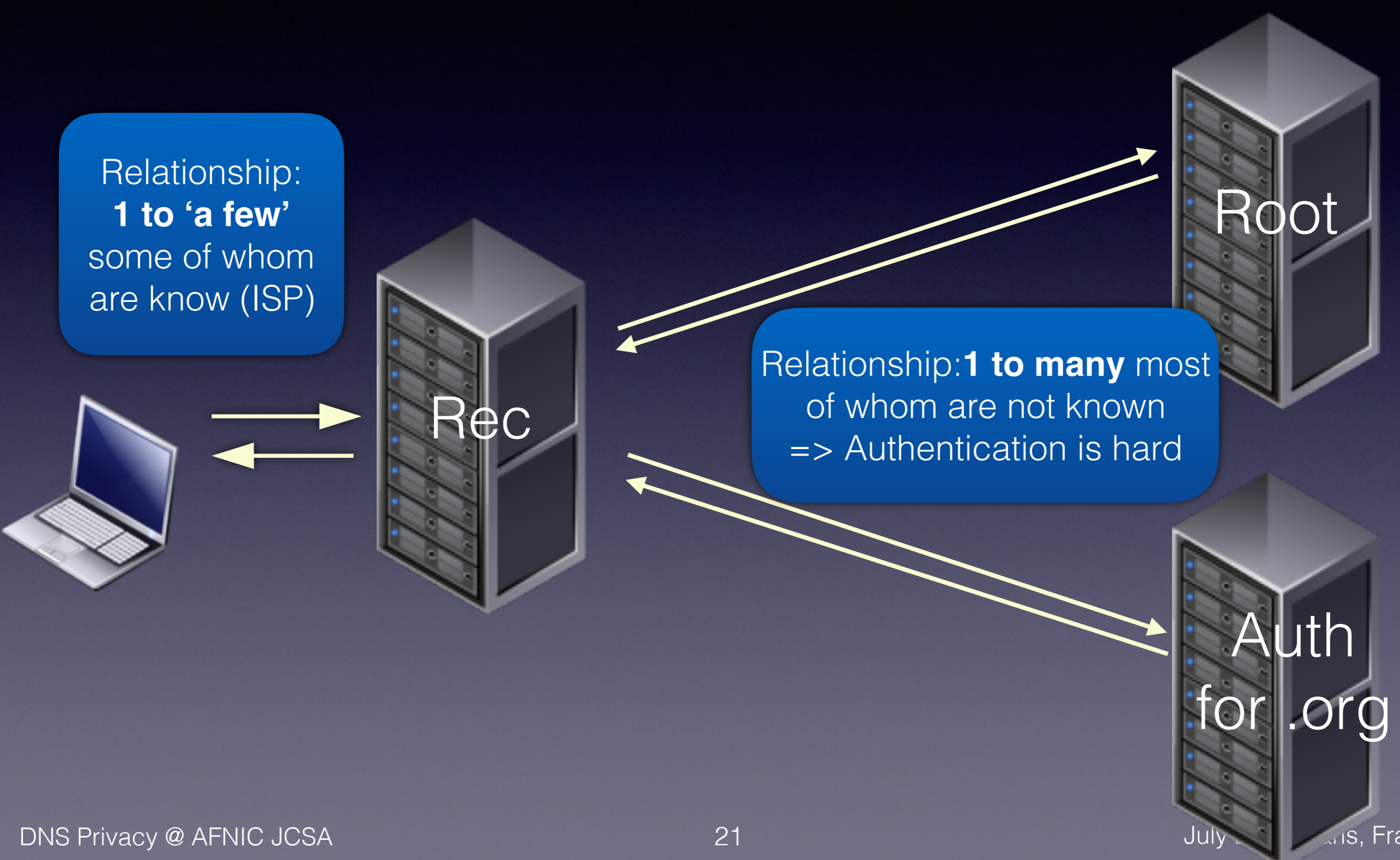
Problem statement: <u>RFC 7626</u>

DNS Privacy Considerations:
Expert coverage of risks throughout DNS ecosystem

- **Rebuts "alleged public nature of DNS data"**

  - The **data** may be public, but a DNS '**transaction**' is not/should not be.

"A typical example from outside the DNS world is: the web site of Alcoholics Anonymous is public; the fact that you visit it should not be."

Stub/Rec Encryption Options

	Pros	Cons
STARTTLS	• Port 53 • Known technique • Incrementation deployment	• Downgrade attack on negotiation • Port 53 - middleboxes blocking? • Latency from negotiation
TLS (new port)	• New DNS port (no interference with port 53) • Existing implementations	• New port assignment • Scalability?
DTLS (new port)	• UDP based • Not as widely used/ deployed	• Truncation of DNS messages (just like UDP) ➡️Fallback to TLS or clear text ❌Can't be standalone solution

Stub/Rec Encryption Options

	Pros	Cons
STARTTLS	• Port 53 • Known technique • Incrementation deployment	• Downgrade attack on negotiation • Port 53 - middleboxes blocking? • Latency from negotiation
TLS (new port)	• New DNS port (no interference with port 53) • Existing implementations	• New port assignment • Scalability?
DTLS (new port)	• UDP based • Not as widely used/ deployed	• Truncation of DNS messages (just like UDP) ➡️Fallback to TLS or clear text ❌Can't be standalone solution

Stub/Rec Encryption Options

	Pros	Cons
STARTTLS	• Port 53 • Known technique • Incrementation deployment	• Downgrade attack on negotiation • Port 53 - middleboxes blocking? • Latency from negotiation
TLS (new port)	• New DNS port (no interference with port 53) • Existing implementations	• New port assignment • Scalability?
DTLS (new port)	• UDP based • Not as widely used/ deployed	• Truncation of DNS messages (just like UDP) ➡️Fallback to TLS or clear text ❌Can't be standalone solution

Encrypted DNS 'TODO' list

1. Get a new port

2. DNS-over-TCP/TLS: Address issues in standards and implementations

3. Tackle authentication of DNS servers (bootstrap problem)

4. What about <u>traffic analysis</u> of encrypted traffic - msg size & timing still tell a lot!

1.Get a new port!

- One does not simply get a new port…

- Oct 2015 - **853** is the magic number

Your request has been processed. We have assigned the following system port number as an early allocations per RFC7120, with the DPRIVE Chairs as the point of contact:

domain-s   853   tcp   DNS query-response protocol run over TLS/DTLS
domain-s   853   udp   DNS query-response protocol run over TLS/DTLS

2. DNS + TCP/TLS?

- DNS-over-TCP history:

    - typical DNS clients do 'one-shot' TCP

    - DNS servers have **very** basic TCP capabilities

    - No attention paid to TCP tuning, robustness

   - Performance tools based on one-shot TCP

2. Fix DNS-over-TCP/TLS

Goal	How?
Optimise set up & resumption	**RFC7413**: TFO Fast Open **RFC5077**: TLS session resumption **TLS 1.3** (0-RTT)
Amortise cost of TCP/TLS setup	**RFC7766** (bis of RFC5966) - March 2016: Client pipelining (not one-shot!), Server concurrent processing, Out-of-order responses **RFC7828:** Persistent connections (Keepalive)
Servers handle many connections robustly	Learn from HTTP world!

Performance (RFC7766)

Client - pipeline requests, keep connection open and handle out-of-order response

Server - concurrent processing of requests sending of out of order responses
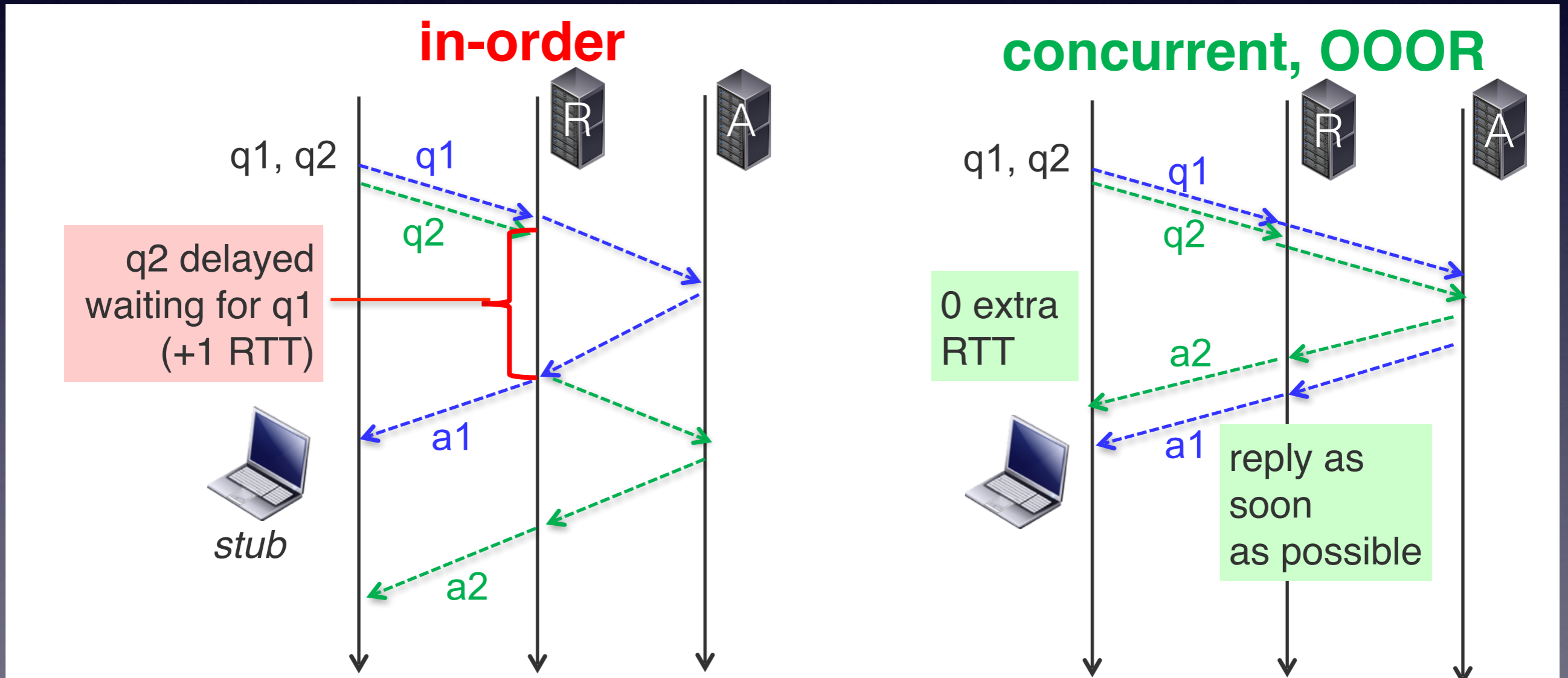
3. Authentication in DNS-over-(D)TLS

2 Usage Profiles:

- Strict

  - "Do or do not. There is no try."

- Opportunistic

  - "Success is stumbling
    from failure to failure
    with no loss of enthusiasm"

3. Authentication in DNS-over-(D)TLS

2 Usage Profiles:

- Strict ————————————▶ (Encrypt & Authenticate) or Nothing

  - "Do or do not. There is no try."

- Opportunistic

  - "Success is stumbling
    from failure to failure
    with no loss of enthusiasm"
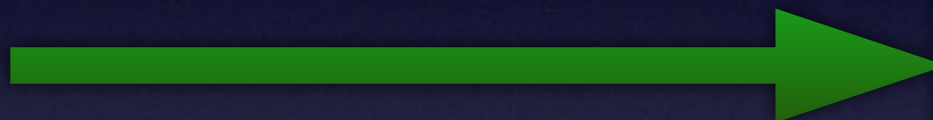
3. Authentication in DNS-over-(D)TLS

2 Usage Profiles:

- Strict ➡ (Encrypt & Authenticate) or Nothing

  - "Do or do not. There is no try."
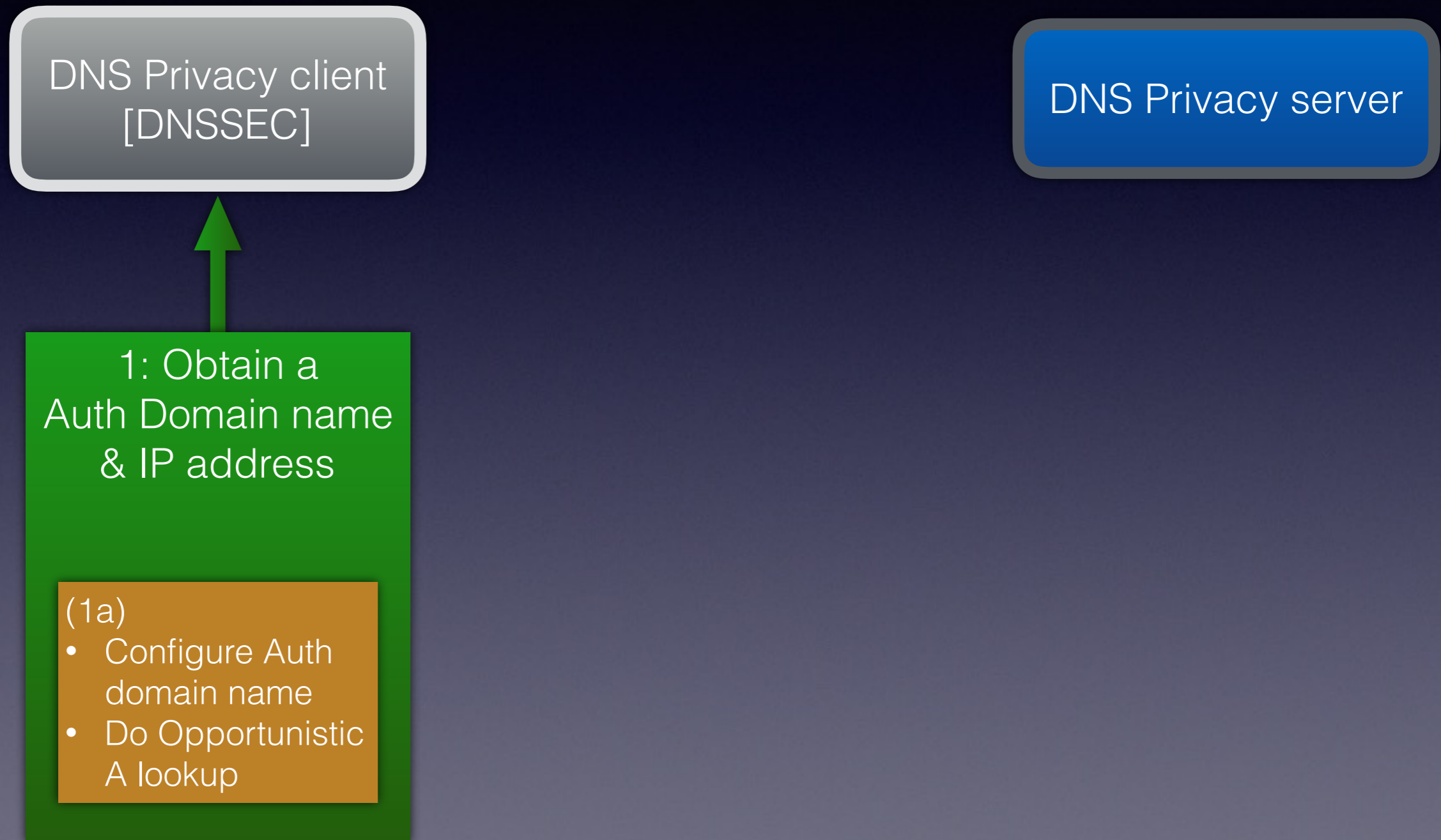
- Opportunistic ➡ Try in order:

  1. Encrypt & Authenticate then
  2. Encrypt then
  3. Clear text

  - "Success is stumbling from failure to failure with no loss of enthusiasm"

3. Authentication in DNS-over-(D)TLS
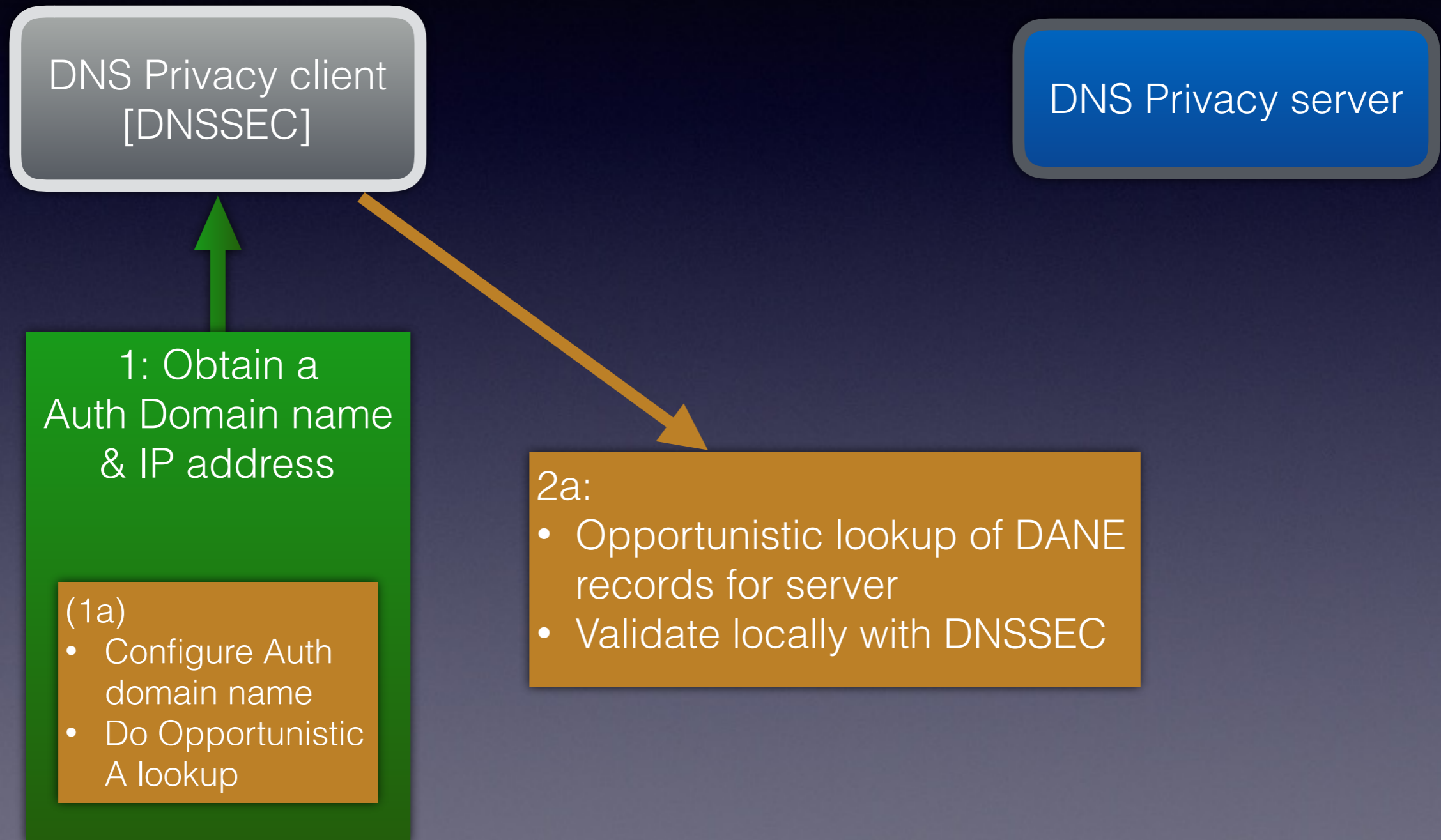
- Authentication based on config of either:

  - Authentication domain name (easier)

  - SPKI pinset (harder)

- Shouldn't DNS use DANE…? Well - even better:

  - I-D: TLS DNSSEC Chain Extension

DNS Auth using DANE

DNS Privacy client
[DNSSEC]

DNS Privacy server

1: Obtain a
Auth Domain name
& IP address

(1a)
- Configure Auth
  domain name
- Do Opportunistic
  A lookup

DNS Auth using DANE

DNS Privacy client
[DNSSEC]

DNS Privacy server

1: Obtain a
Auth Domain name
& IP address

(1a)
• Configure Auth
domain name
• Do Opportunistic
A lookup

2a:
• Opportunistic lookup of DANE
records for server
• Validate locally with DNSSEC

DNS Auth using DANE

DNS Privacy client [DNSSEC]

DNS Privacy server

1: Obtain a Auth Domain name & IP address

(1a)
- Configure Auth domain name
- Do Opportunistic A lookup

2a:
- Opportunistic lookup of DANE records for server
- Validate locally with DNSSEC

DNS Auth using DANE

DNS Privacy client [DNSSEC] ←— TLS —→ **DNS Privacy server**

1: Obtain a Auth Domain name & IP address

(1a)
- Configure Auth domain name
- Do Opportunistic A lookup

2a:
- Opportunistic lookup of DANE records for server
- Validate locally with DNSSEC

DNS Auth using DANE

DNS Privacy client
[DNSSEC]

TLS

DNS Privacy server

1: Obtain a
Auth Domain name
& IP address

(1a)
• Configure Auth domain name
• Do Opportunistic A lookup

2a:
• Opportunistic lookup of DANE records for server
• Validate locally with DNSSEC

TLS DNSSEC Chain Extension

DNS Privacy client
[DNSSEC]

DNS Privacy server

1: Obtain a
Auth Domain name
& IP address

(1a)
• Configure Auth
  domain name
• Do Opportunistic
  A lookup

TLS DNSSEC Chain Extension

DNS Privacy client [DNSSEC]

DNS Privacy server

1: Obtain a Auth Domain name & IP address

(1a)
- Configure Auth domain name
- Do Opportunistic A lookup

0 (or 2): Obtains DANE records for itself!

TLS DNSSEC Chain Extension

DNS Privacy client [DNSSEC]

Client Hello:
TLS DNSSEC Chain Ext

DNS Privacy server

1: Obtain a Auth Domain name & IP address

(1a)
• Configure Auth domain name
• Do Opportunistic A lookup

0 (or 2): Obtains DANE records for itself!

TLS DNSSEC Chain Extension

Client Hello:
TLS DNSSEC Chain Ext

DNS Privacy client
[DNSSEC]

Server Hello:
Server DANE records

DNS Privacy server

1: Obtain a
Auth Domain name
& IP address

(1a)
• Configure Auth
  domain name
• Do Opportunistic
  A lookup

0 (or 2): Obtains
DANE records for
itself!

TLS DNSSEC Chain Extension

DNS Privacy client
[DNSSEC]

Client Hello:
TLS DNSSEC Chain Ext

DNS Privacy server

Server Hello:
Server DANE records

1: Obtain a
Auth Domain name
& IP address

(1a)
- Configure Auth domain name
- Do Opportunistic A lookup

0 (or 2): Obtains DANE records for itself!

TLS DNSSEC Chain Extension

DNS Privacy client [DNSSEC]

Client Hello:
TLS DNSSEC Chain Ext

Server Hello:
Server DANE records

DNS Privacy server

1: Obtain a
Auth Domain name
& IP address

(1a)
• Configure Auth
  domain name
• Do Opportunistic
  A lookup

• Reduces Latency
• Eliminates need for
  intermediate recursive

0 (or 2): Obtains
DANE records for
itself!

DPRIVE Solution Documents
(stub to recursive)

Document	Date	Topic
RFC7858	May 2016	DNS-over-TLS
RFC7830	May 2016	**EDNS0 Padding Option**
RFC8094	Feb 2017	DNS-over-DTLS
draft-ietf-dprive-dtls-and-tls-profiles	IESG LC	Authentication for DNS-over-(D)TLS

*Category: Experimental

What about Recursive to Authoritative?

- I-D: Next step for DPRIVE: resolver-to-auth link
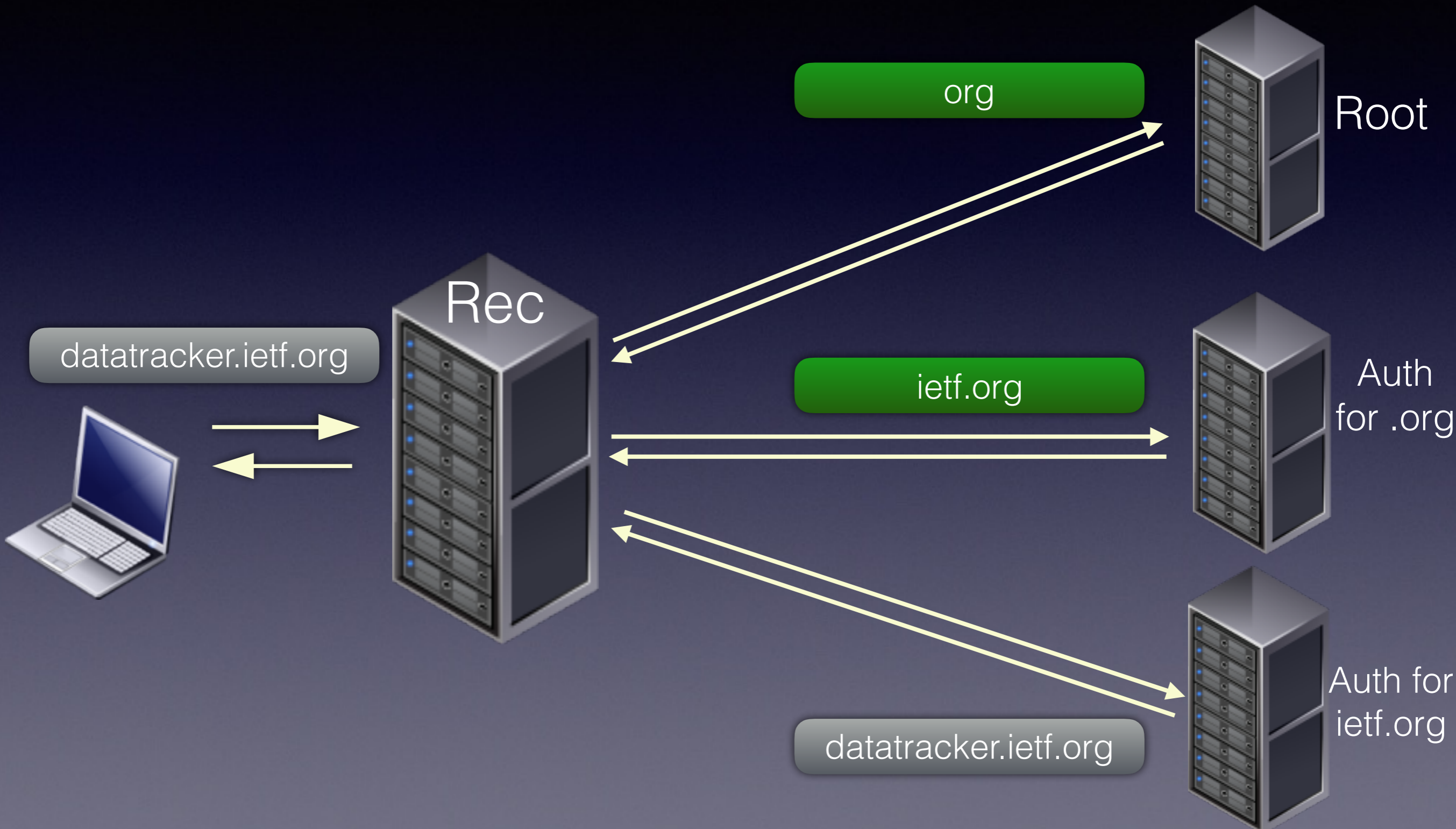
  - Presents 6 authentication options

- DPRIVE - Re-charter…

- Data on DNS-over-(D)TLS

WE SHOULDN'T BE EXPLORING OTHER PLANETS UNTIL WE'VE SOLVED ALL OUR PROBLEMS HERE ON EARTH.

SOUNDS REASONABLE. SO, WHAT'S THE TIMELINE ON "SOLVING ALL PROBLEMS"?

TEN YEARS? FIFTEEN?
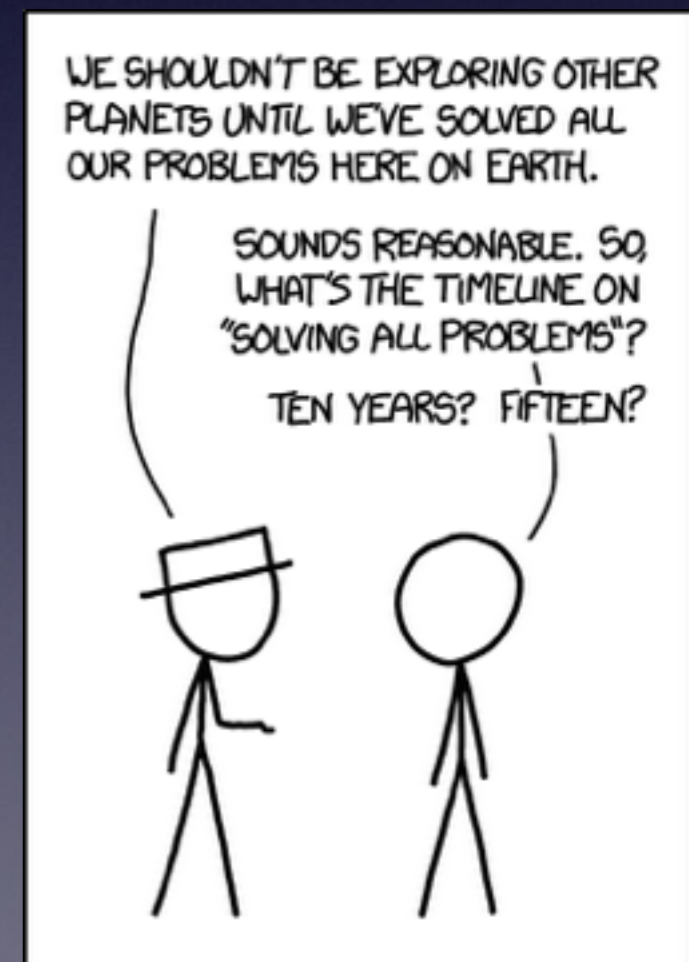
Other work….

DNS Disclosure Example 1

Leaks information → datatracker.ietf.org

Root

datatracker.ietf.org

Rec

datatracker.ietf.org

Auth for .org

datatracker.ietf.org

Auth for ietf.org
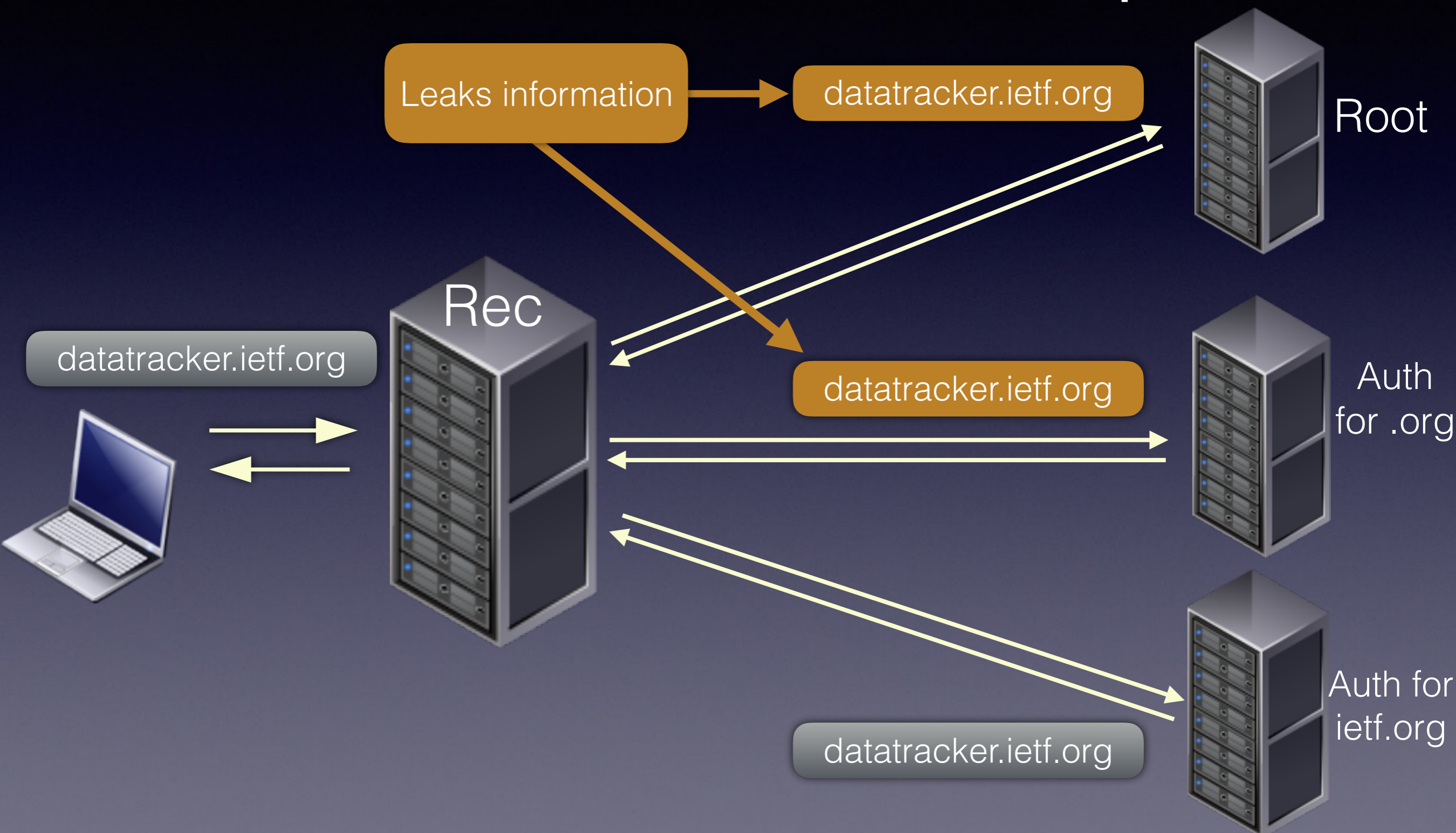
RFC7816: QNAME Minimisation

org

Root

Rec

datatracker.ietf.org

ietf.org

Auth for .org

datatracker.ietf.org

Auth for ietf.org

DNS Data handling

- Do you read the small print of your ISPs contract?

- More work/research needed in this area

  - **Monitoring** of government policy and practice

  - **Transparency** from providers on policy and breaches

  - Methods for **de-identification** of user data (e.g. DITL)

  - '**PassiveDNS**' data used for research/security

DNS Data handling

- Do you read the small print of your ISPs contract?

- More wo

  - **Monit**   ctice

  - **Trans**   nd breaches

  - Metho   a (e.g. DITL)

  - '**PassiveDNS**' data used for research/security

Not always a technical solution:
Needs more work

DNS-over-HTTP(S)

Avoids e.g. port 853 blocking

- Google: DNS-over-HTTPS (non-standard)

- Standards are in flux (many drafts….)

  - DNS wire-format over HTTP (tunnelling)

    Implementations exist

  - DNS over HTTPS (query origination)

    Mix HTTPS/2 and DNS on one connection

DNS-over-QUIC

- DNS over dedicated QUIC connections

  - QUIC is a developing open source protocol (from Google) that runs over UDP (HTTPS/2-like)

  - **~35% of Google's egress traffic** (~7% of Internet traffic)

  - **Reliable**, low latency, performant

  - Source address validation, no MTU limit

  - **Encrypted**

Risk Mitigation Matrix

Risk	In-Flight		At Rest	
	Stub => Rec	**Rec => Auth**	**At Recursive**	**At Authoritative**
Passive monitoring	**Encryption (e.g. TLS, HTTPS)**	**QNAME Minimization**		
Active monitoring	**Authentication & Encryption**			
Other Disclosure Risks e.g. Data breaches			**Data Best Practices (Policies) e.g. De-identification**	

DNS Service Discovery

DNS Service Discovery

- Devices advertise services on network (DNS, mDNS) - leakage can be global

- Other devices then discover the service and use it

DNS Service Discovery

- Devices advertise services on network (DNS, mDNS) - leakage can be global

- Other devices then discover the service and use it

Alice's Images   . _imageStore._tcp . local
Alice's Mobile Phone   . _presence._tcp   . local
Alice's Notebook   . _presence._tcp   . local

DNS-SD Privacy

- Advertising leaks information about:

  - User - 'name', devices, services (user tracking)

  - Devices - services & attributes (port, priorities)

    - Device fingerprinting possible

    => Software or specific device identification

- Discovery leaks info about preferred services

DNS-SD Privacy

- Advertising leaks information about:

  - User - 'name', devices, services (user tracking)

  - Devices - services & attributes (port, priorities)

    - Device fingerprinting possible

  => Software or specific device identification

- Discovery leaks info about preferred services

DNS Privacy Implementation Status

dnsprivacy.org
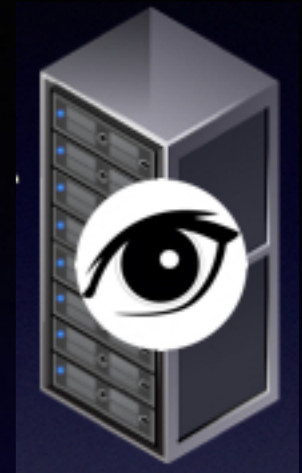
- DNS Privacy Project homepage

- **Who?** Sinodun, NLnet Labs, Salesforce,…
  (plus various grants and individual contributions)

- **What?** Point of reference for DNS Privacy services

  - Quick start guides for operators & end users

  - Ongoing work - presentations, IETF, Hackathons

  - Tracking of DNS-over-TLS experimental servers

Recursive implementations

Features		Recursive resolver		
		Knot Res	**Unbound**	**BIND**
TCP/TLS Features	**TCP fast open**	Dark Green	Dark Green	Yellow
	Process pipelined queries	Dark Green	Dark Green	Dark Green
	Provide OOOR	Dark Green	Yellow	Dark Green
	EDNS0 Keepalive	Grey	Yellow	Yellow
TLS Features	**TLS on port 853**	Dark Green	Dark Green	Purple
	Provide server certificate	Dark Green	Dark Green	Purple
	EDNS0 Padding	Dark Green	Grey	Grey
Rec => Auth	**QNAME Minimisation**	Dark Green	Dark Green	Yellow

■ Dark Green: Latest stable release supports this
■ Light Green: Patch available
■ Yellow: Patch/work in progress, or requires building a patched dependency
■ Purple: Workaround available
■ Grey: Not applicable or not yet planned

Alternative server side solutions

- Pure TLS load balancer

  - <u>NGINX, HAProxy</u>

  - <u>BIND article</u> on using stunnel

  > Disadvantages
  > - DNS specific access control is missing
  > - pass through of edns0-tcp-keepalive option

- <u>dnsdist</u> from PowerDNS would be great…

  - But no support yet but requested: <u>#3980</u>

Stub implementations

Features		Stub			
		getdns (stubby)	kdig	BIND (dig)	ldns
TCP/TLS Features	TCP fast open	🟩	🟩	🟨	🟩
	Connection reuse	🟩	🟩	🟩	🟩
	Pipelining of queries	🟩	🟩	🟩	⬜
	Process OOOR	🟩	🟩	🟩	⬜
	EDNS0 Keepalive	🟩	⬜	🟨	⬜
TLS Features	TLS on port 853	🟩	🟩	⬜	🟩
	Authentication of server	🟩	🟩	⬜	⬜
	EDNS0 Padding	🟩	🟩	⬜	⬜

Dark Green: Latest stable release supports this
Light Green: Patch available
Yellow: Patch/work in progress
Grey: Not applicable or not yet planned

Implementation Status Summary

- Increasing uptake of better DNS-over-TCP, QNAME minimisation

- Several implementations of DNS-over-TLS

- None yet of DNS-over-DTLS

- BII has <u>DNS-over-HTTP implementation</u>

DNS Privacy Deployment Status
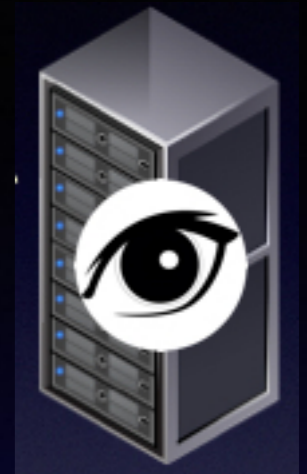
Server monitoring

Project dnsprivacy-monitoring

* Green indicates success

* Red indicates failed test (this might result from non DNS related issues such server being off line, blocking from the probe location, etc.) Note that the 'Strict mode' tests could fail for a number of reasons including incorrect credentials, self-signed certificates for name only authentication, incompatible TLS version or Cipher suites, etc. The console log of the test may give more information.

* Grey indicates test not run (e.g. due to lack of available transport or the lack of the SPKI pin)

Authentication information is taken from https://dnsprivacy.org/wiki/display/DP/DNS+Privacy+Test+Servers
These tests use Stephane Bortzmeyer's nagios plugin - see https://github.com/bortzmeyer/monitor-dns-over-tls

Configuration Matrix		Responds over TLS	Strict mode - Name only	Strict mode - SPKI only	Certificate expiry > 0 days	Certificate expiry > 14 days	QNAME minimisation used
getdnsapi.net	v6	✓	✓	✓	✓	✓	✓
	v4	✓	✓	✓	✓	✓	✓
dnsovertls.sinodun.com	v6	✓	✓	✓	✓	✓	!
	v4	✓	✓	✓	✓	✓	!
dnsovertls1.sinodun.com	v6	✓	✓	✓	✓	✓	!
	v4	✓	✓	✓	✓	✓	!
dns.cmrg.net	v6	✓	✓	✓	✓	✓	✓
	v4	✓	✓	✓	✓	✓	!
tls-dns-u.odvr.dns-oarc.net	v6	✓	!	!	✓	✓	!
	v4	✓	!	!	✓	✓	!
dns-resolver.yeti.eu.org	v6	✓	✓	✓	✓	✓	✓
	v4	●	●	●	●	●	●
yeti-rr.datev.net	v6	✓	✓	✓	✓	✓	✓
	v4	●	●	●	●	●	●
unicast.censurfridns.dk	v6	✓	✓	●	✓	✓	!
	v4	✓	✓	●	✓	✓	!
dns-tls.openbsd.se	v6	●	●	●	●	●	●
	v4	✓	✓	✓	✓	✓	!

Stubby

- A privacy enabling stub resolver: <u>User Guide</u>

- Available in <u>getdns</u> (1.1.1 release)

  - Run as daemon handling requests

  - Configure OS DNS resolution to point at *localhost*

  - DNS queries then proxied over TLS

  - Comes with config for experimental servers

Stubby Status

- Command tool still prototype - for 'advanced' users

  - Supports name and SPKI pinset authentication

  - Strict and Opportunistic profiles

- Homebrew formula, docker image and macOS UI on the way…..

Stubby Usability

- DNS Privacy is a new paradigm for end users

- End users are a new paradigm for DNS people!

- '**Usable Security**': Good GUIs aren't enough - users still struggle with the basics if they don't understand what they are doing (HTTPS, PGP, DNSSEC)

- DNS Privacy uptake critically dependant on clients being usable + successful

Key challenges

1. Awareness!

2. Clients: OS integration of (more) client solutions

3. Usable client solutions for non-technical users

4. Increased deployment (anycast deployments)

5. Operator transparency in DNS data handling

6. Recursive to Authoritative….

Summary

- DNS Privacy is a real problem and more relevant than ever

- Active work on the large solution space

- Can use DNS Privacy today using Stubby & current experimental recursive servers

- More DNS Privacy services on the way…

Thank you!

Any Questions?

dnsprivacy.org