dnsprivacy.net

A project to support deployment of DNS-over-TLS services

Sara Dickinson, Sinodun
sara@sinodun.com

OARC 26, Madrid

May 2017

DNS Privacy activity

Jun 2013	Snowdon revelations
May 2014	**IETF reaction - RFC 7258**: “**Pervasive Monitoring is an attack on the privacy of Internet users and organisations**.”
Mar 2014	DPRIVE Working Group Formed
Aug 2015	RFC 7626 -DNS Privacy Considerations
May 2016	RFC 7858 - DNS-over-TLS Specification
Nov 2016	IETF EDU: DNS Privacy Tutorial

DNS sent in clear text
NSA: ‘MORECOWBELL’

RFC 7626 - DNS Privacy Considerations

- Problem statement: Expert coverage of risks throughout DNS ecosystem (no privacy in design)
- **Rebuts "alleged public nature of DNS data"**
  - The **data** may be public, but a DNS '**transaction**' is not/should not be.

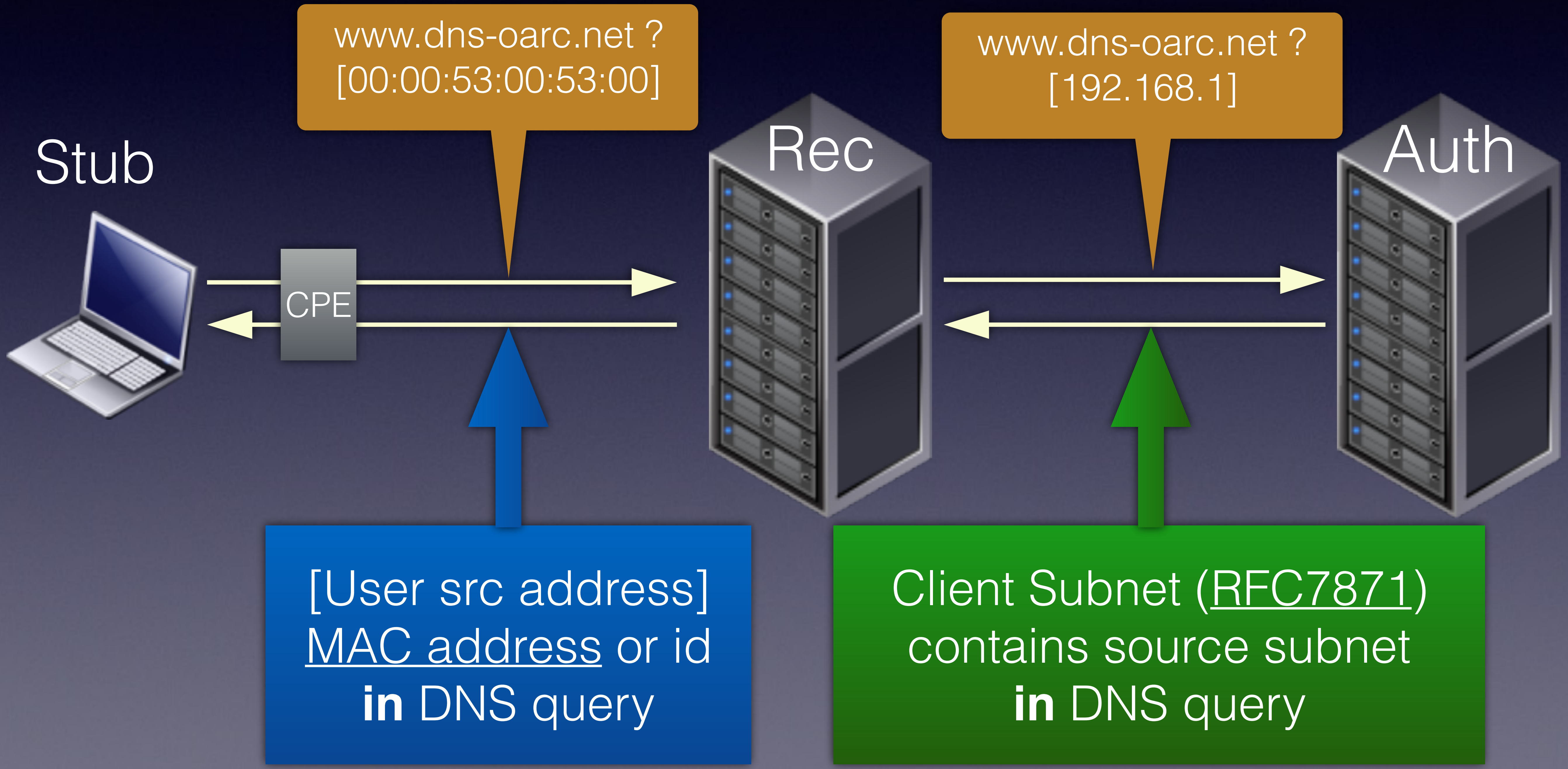
> "A typical example from outside the DNS world is: the web site of Alcoholics Anonymous is public; the fact that you visit it should not be."

- EDNS0 enables user data to be embedded in DNS

DNS Risk Matrix

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

DNS Disclosure Example 1



Stub

CPE

www.dns-oarc.net ?
[00:00:53:00:53:00]

Rec

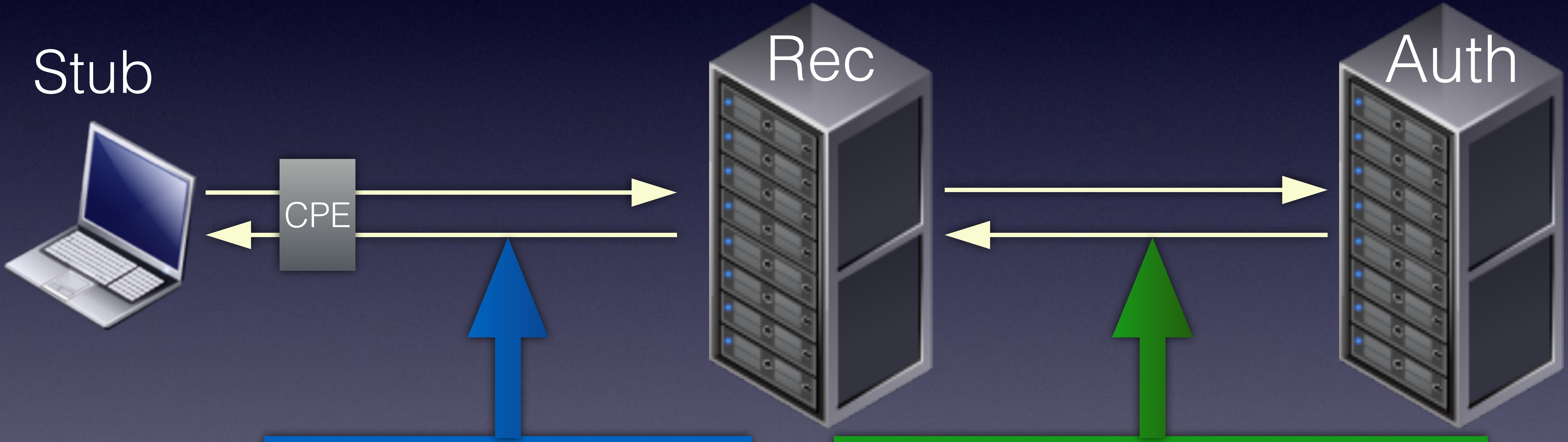
www.dns-oarc.net ?
[192.168.1]

Auth

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

Client Subnet (RFC7871)
contains source subnet
in DNS query

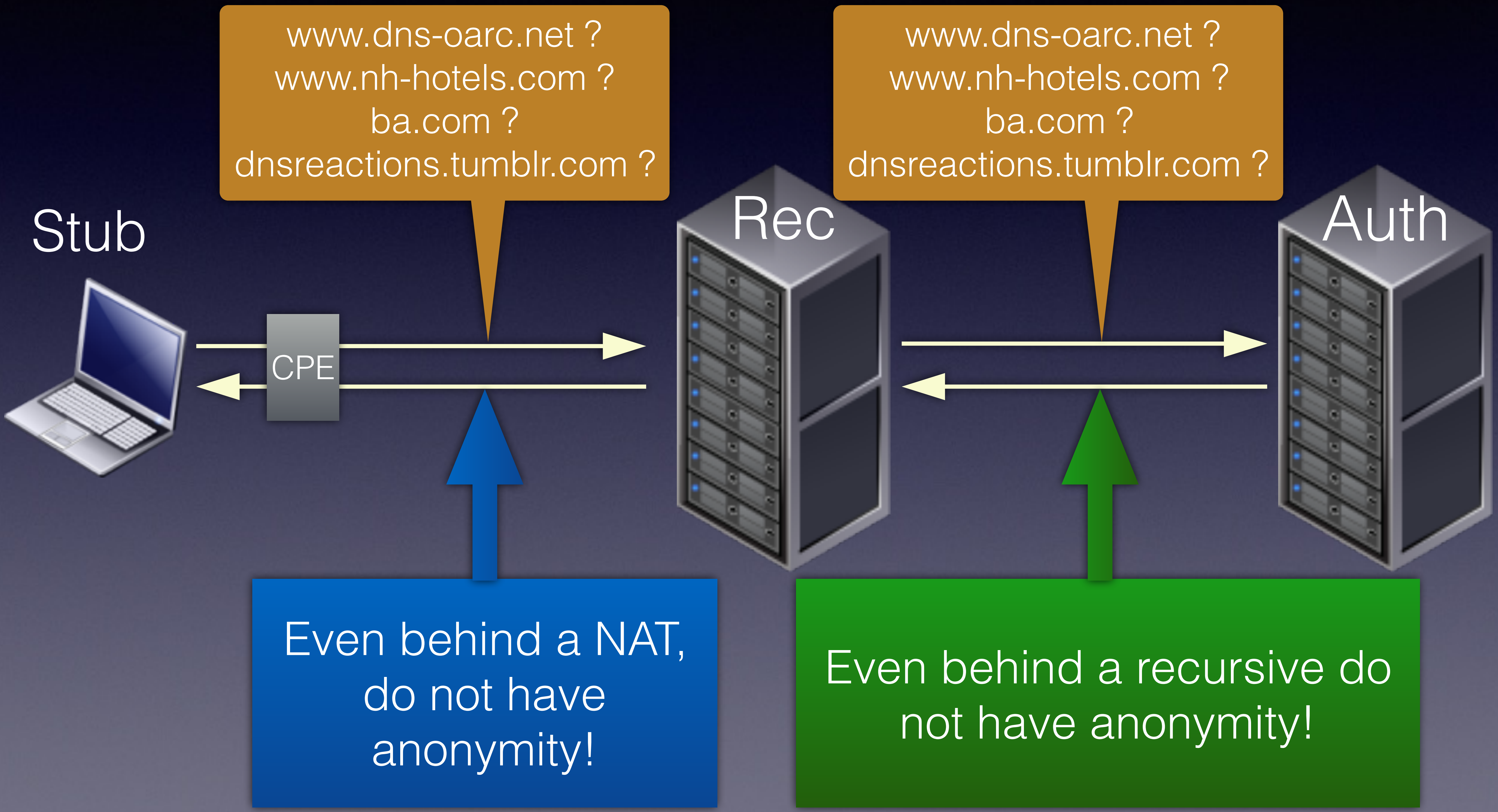
DNS Disclosure Example 1



Even behind a NAT, do not have anonymity!

Even behind a recursive do not have anonymity!

DNS Disclosure Example 1



www.dns-oarc.net ?
www.nh-hotels.com ?
ba.com ?
dnsreactions.tumblr.com ?

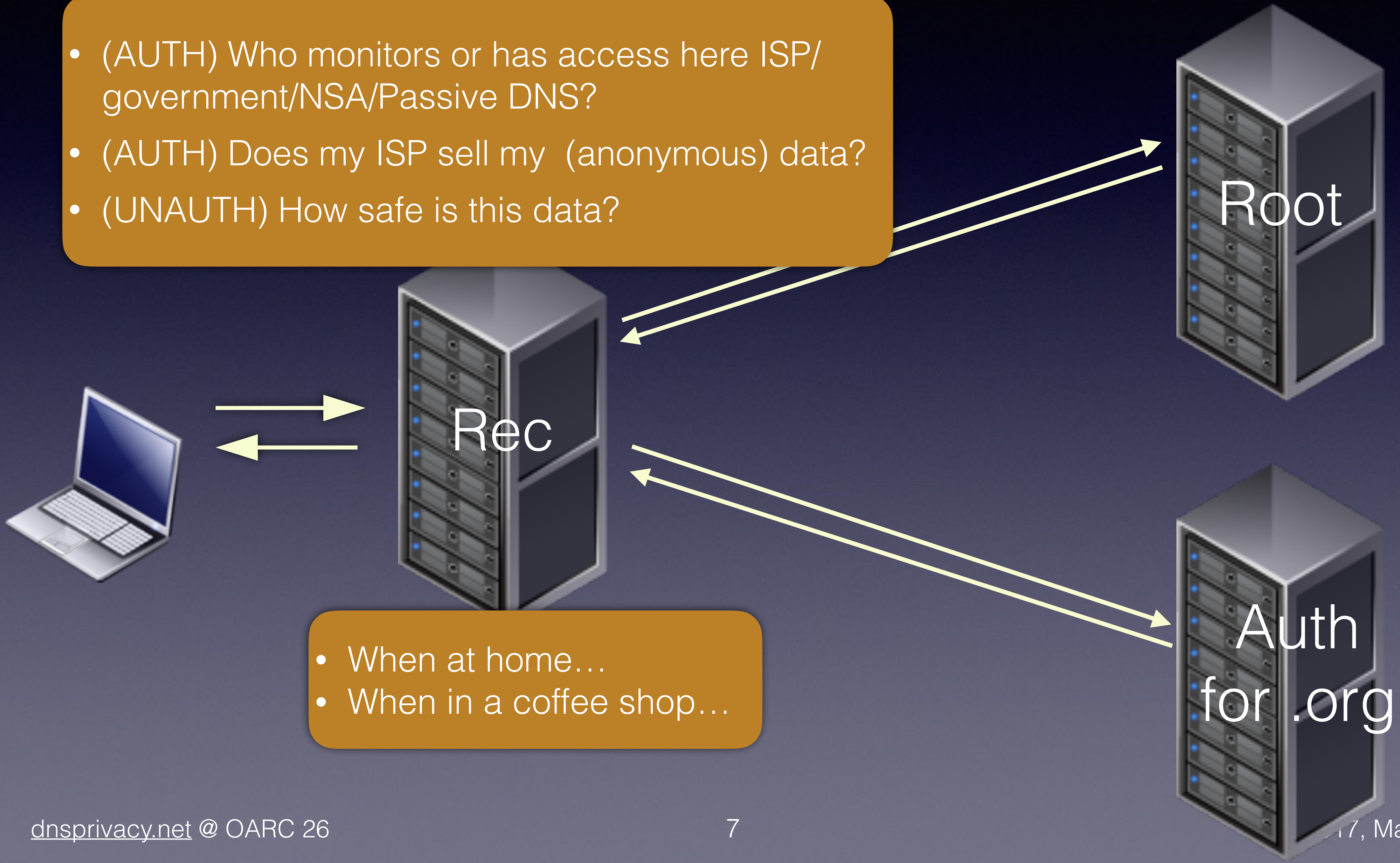
www.dns-oarc.net ?
www.nh-hotels.com ?
ba.com ?
dnsreactions.tumblr.com ?

Even behind a NAT, do not have anonymity!

Even behind a recursive do not have anonymity!

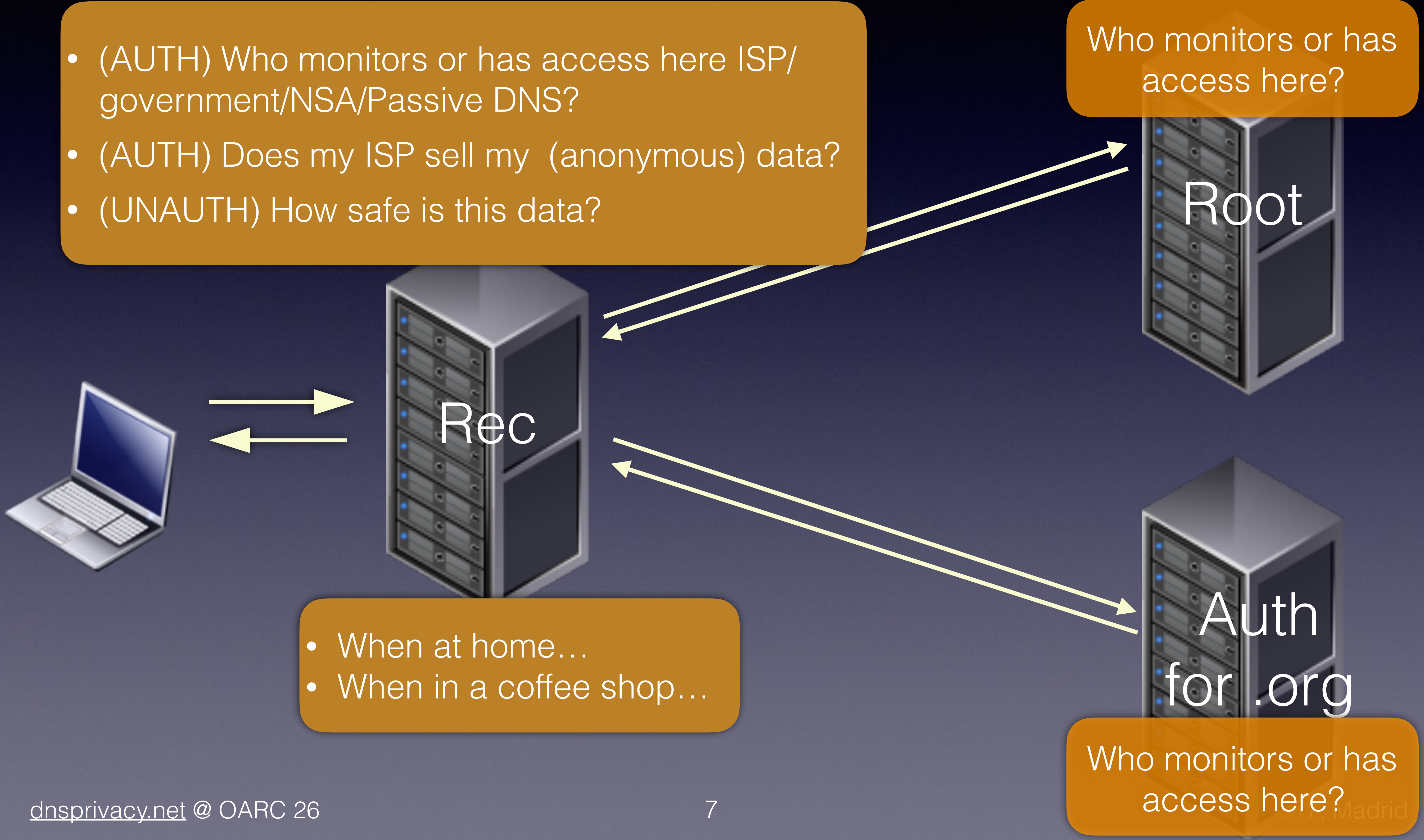
DNS Disclosure Example 2

- (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?



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

DNS Disclosure Example 2



- (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?

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

Who monitors or has access here?

DPRIVE WG

- DPRIVE WG create in 2014

Charter: Primary Focus is
Stub to recursive

- **RFC7858 (2016)** - DNS-over-TLS, port 853 assigned
- **Internet Draft** on authenticating DNS Privacy Server
- Supporting work on **DNS-over-TCP**, **QNAME min**
- WG now considering Recursive to Authoritative

Risk Mitigation Matrix

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

dnsprivacy project

- **What?** Central point of reference for DNS Privacy services
- **Who?** NLnet Labs, Salesforce, Sinodun, No Mountain Software (plus various grants and individual contributions)
- **dnsprivacy.net** - Supporting deployment of DNS Privacy services. **Target audience:** Operators
- **dnsprivacy.org** - Supporting end users of DNS Privacy services. **Target audience:** Technical Users, Activists, … general public.

dnsprivacy project

- **What?** Central point of reference for DNS Privacy services
- **Who?** NLnet Labs, Salesforce, Sinodun, No Mountain Software (plus various grants and individual contributions)
- **dnsprivacy.net** - Supporting deployment of DNS Privacy services. **Target audience:** Operators
- **dnsprivacy.org** - Supporting end users of DNS Privacy services. **Target audience:** Technical Users, Activists, … general public.

A work in progress: both under dnsprivacy.org at the moment!

RECURSIVE

Server Side Solutions

- dnsprivacy.net has material on:
  - Recursive implementations
    - *Unbound, Knot Resolver* support DNS-over-TLS
    - Status of supporting TCP/TLS features
  - Using a pure TLS load balancer
    - NGINX, HAProxy, *stunnel, docker image*
  - Let’s Encrypt certificate management automation

RECURSIVE

Experimental!

DNS-over-TLS Test Servers

Hosted by	Software
NLnet Labs	Unbound
OARC	Unbound
Surfnet/Sinodun	Bind + HAProxy Bind + nginx
dkg.cmrg.net	Knot Resolver

Yeti, UncensoredDNS, Lorraine data network, …

Find details at: DNS Test Servers

Stubby

- A privacy enabling stub resolver
  - How to build and use Stubby
- Available in 1.1.0 release of getdns
  - Run as daemon handling requests
  - Configure OS DNS resolution to point at 127.0.0.1
  - Comes pre-configured with DNS privacy servers

dnsprivacy.net Work In Progress

- Setting up monitoring page for DNS Servers
  (they are experimental, after all!)
- Tools to aid deployment
  (docker images, benchmarking tools, monitoring software)
- Engage with operators to
  - Increase number and diversity of DNS Privacy servers
  - Gather information and develop policies
  - Produce a BCP on DNS Privacy operation and data handling

Thank you!

DNS Privacy Tutorial

dnsprivacy.net
dnsprivacy.org

Any Questions?