
cisco Live!
ALL IN

The bridge to possible

The Evolution of DNS Security

Christian Clasen – Technical Leader, Cloud Security TME
@xianclasen

BRKSEC-2051

Cisco Webex App

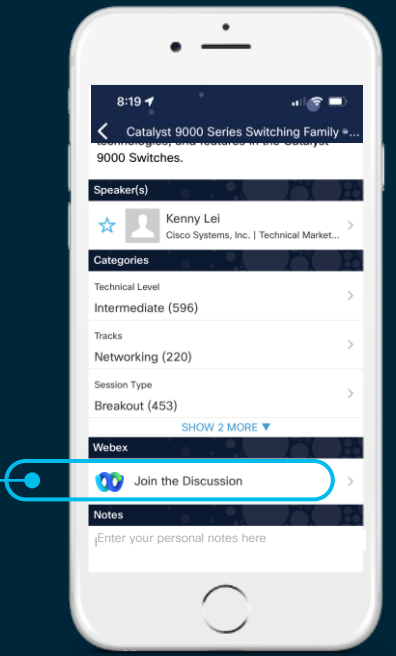
Questions?

Use Cisco Webex App to chat
with the speaker after the session

How

1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until June 17, 2022.



https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-2051

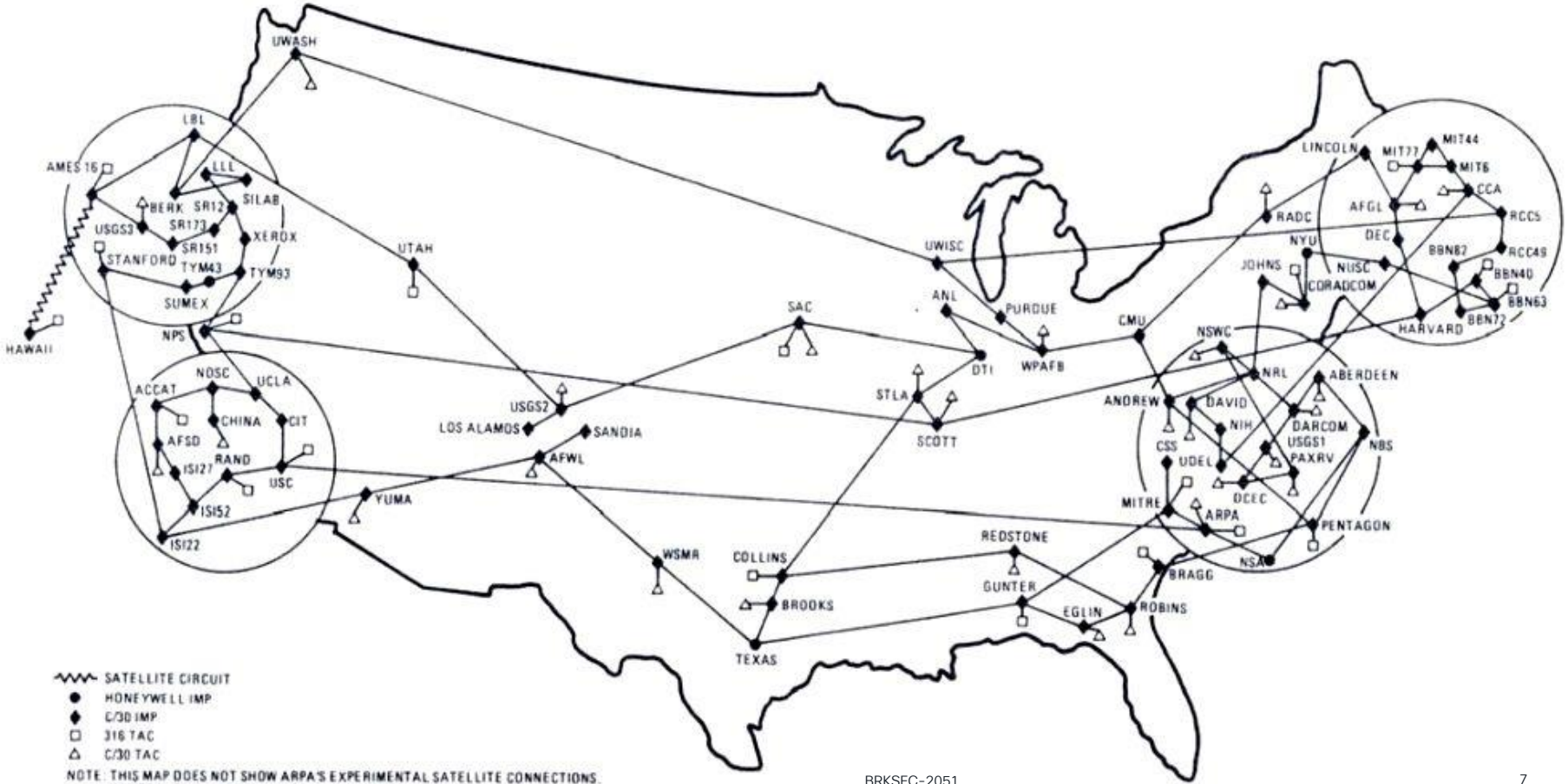
```
me@intro:~$ whoami | jq

    {
        "name":       "christian clasen",
        "title":      "technical leader",
        "org":        "cloud security tme",
        "family":{
                "wife":  ["lindsey"],
                "kids":  ["conrad", "evan", "reid"],
                "dogs":  ["connor"],
                "cats":  ["eva", "ansel"]
                },
        "hobbies":    ["music", "beer", "outdoors"]
    }

me@intro:~$ history | tail

1332 Network and Systems Administrator
1333 Security Lead - MSP
1334 Web Security TAC engineer
1335 Web Security TME
1336 API-Based email security
1337 Cloud Security TME
```

Agenda

- DNS Overview
- Vulnerabilities and Abuses
- DNSSEC and DNSCrypt
- DoT / DoH

DNS Overview

ARPANET GEOGRAPHIC MAP, FEBRUARY 1983



Hosts table

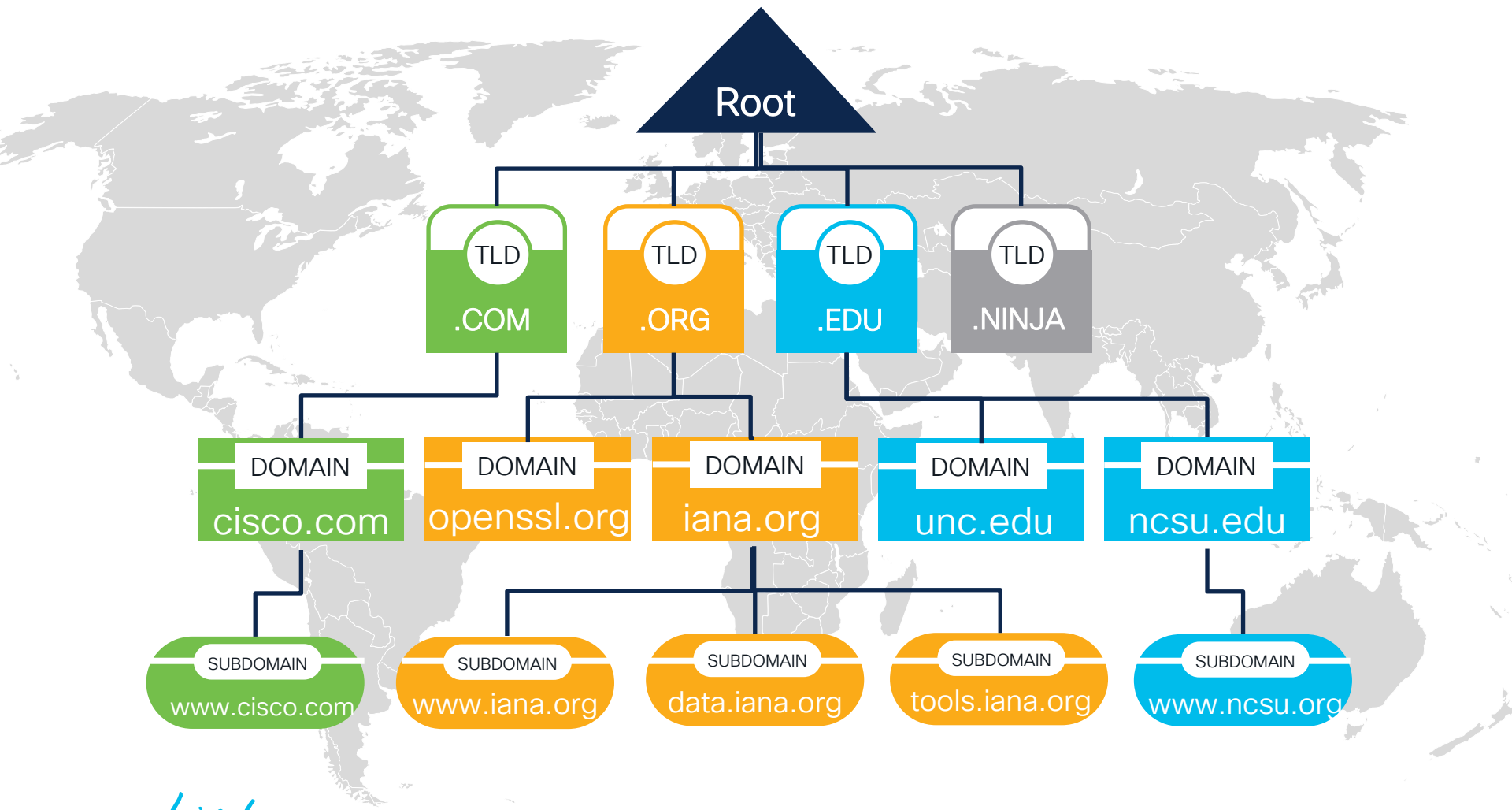
- Maintained by Stanford Research Institute
- Required manual lookup
- Error prone

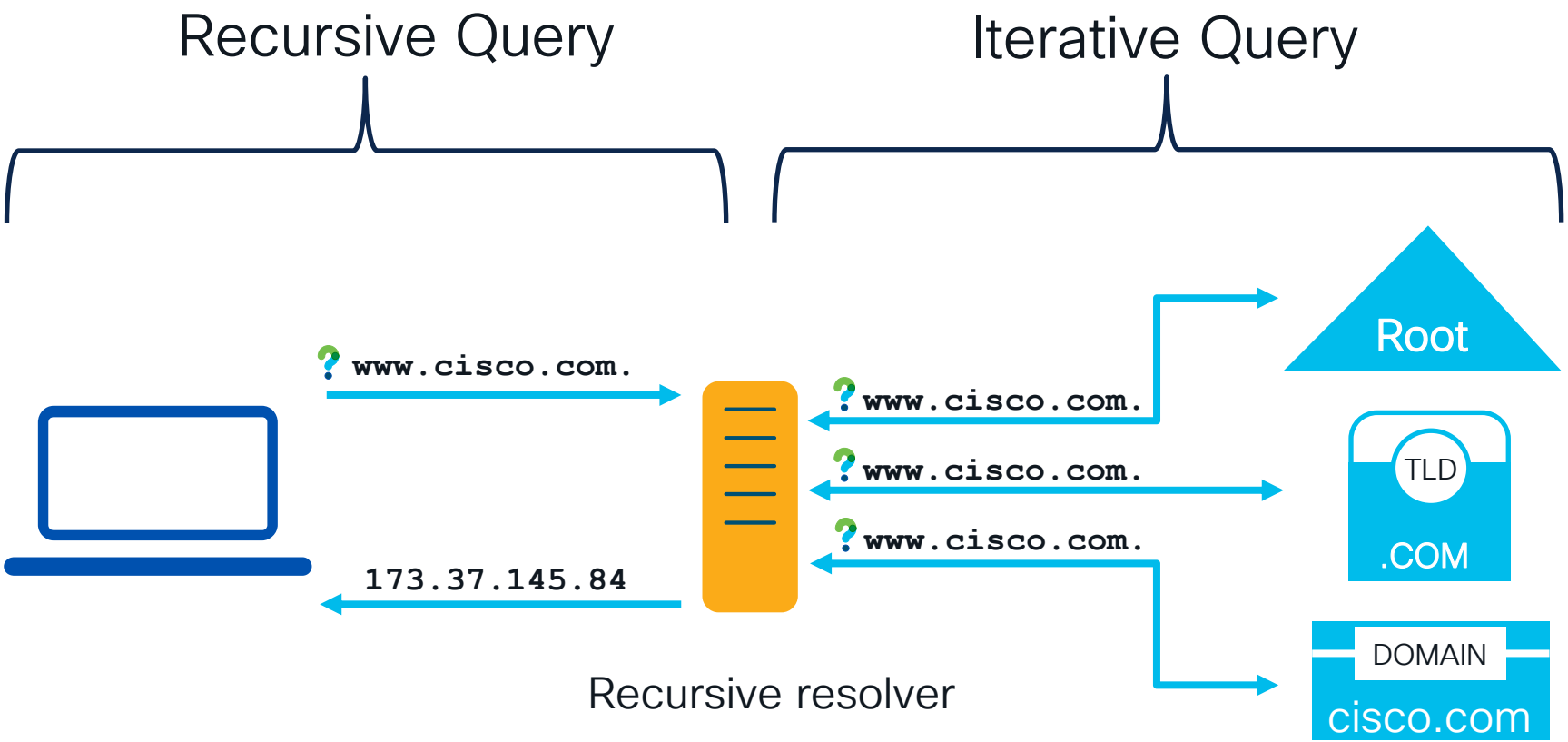
"...operational nightmare."
-Craig Partridge

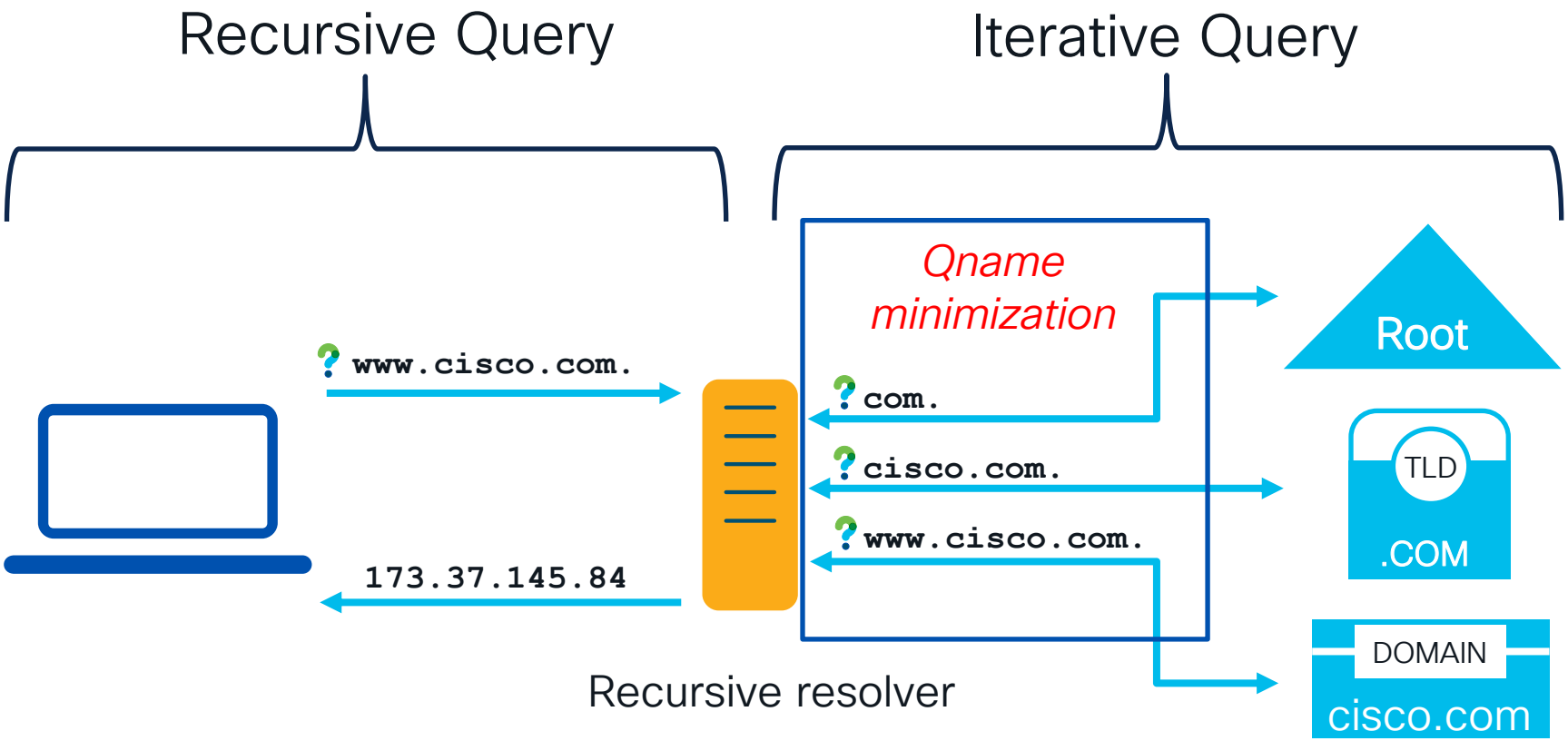
Domain Name System

- Created by Paul Mockapretris
- RFC 882/883 (1034/1035)
- Hierarchical, distributed
- First TLDs established in 1984

NOTIFY and IXFR







"Addresses, and the routing of address prefixes, is increasingly a marginal activity. ...The glue of today's Internet is the name space... The way that we invest trust in the space is now the core conversation of today's Internet."

Geoff Huston, Chief Scientist at the Asia Pacific Network Information Centre (APNIC)

Vulnerabilities and Abuses

Classes of DNS attacks

Cache Poisoning

- Query ID guessing
- Mitigated in 1998
- Still possible but unlikely

Spoofing / Hijacking

- Very easy to do
- Difficult to detect
- ISPs regularly hijack DNS

Denial of Service

- Amplification attacks
- UDP makes this possible
- Small query, big reply

Snooping / fingerprinting

- Plain-text queries and replies
- Privacy concern
- ISPs regularly snoop DNS

Classes of DNS attacks

Cache Poisoning

- Query ID guessing
- Mitigated in 1998
- Still possible but unlikely

Spoofing / Hijacking

- Very easy to do
- Difficult to detect
- ISPs regularly hijack DNS

~~Privacy~~ ~~Integrity~~ ~~Authenticity~~

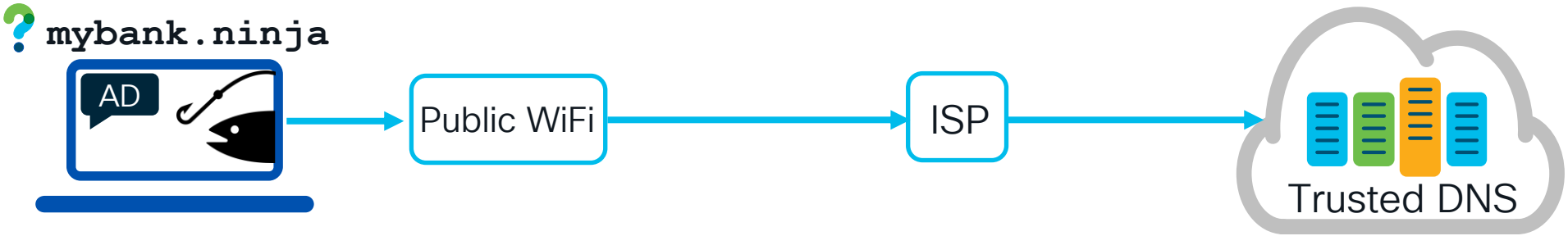
Denial of Service

- Amplification attacks
- UDP makes this possible
- Small query, big reply

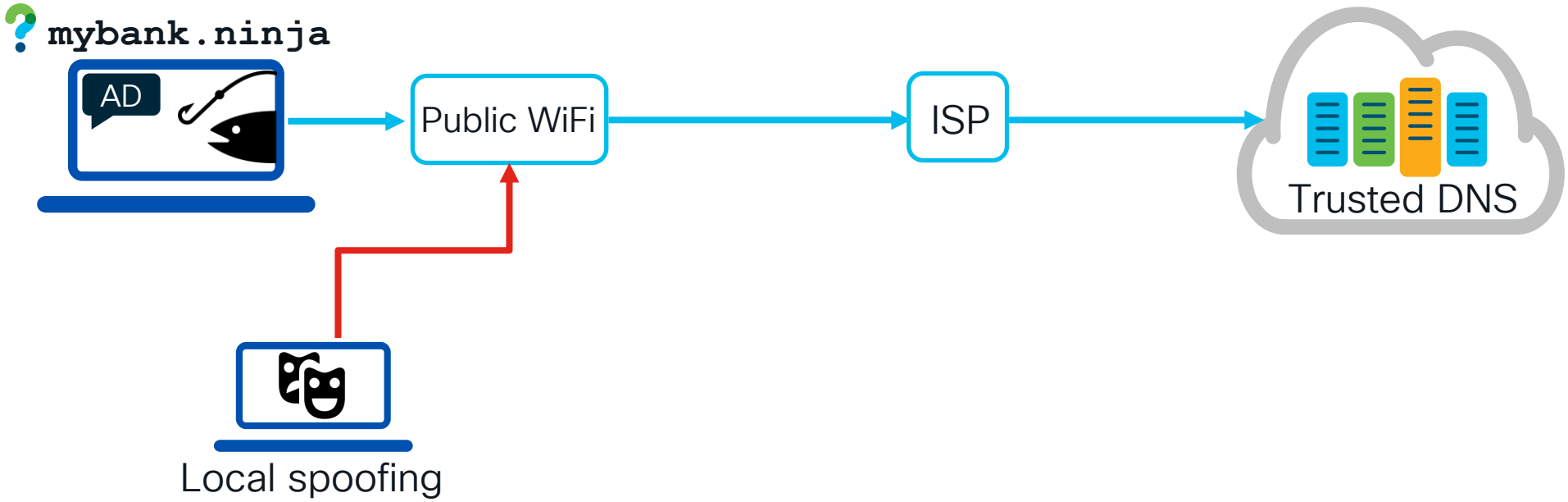
Snooping / fingerprinting

- Plain-text queries and replies
- Privacy concern
- ISPs regularly snoop DNS

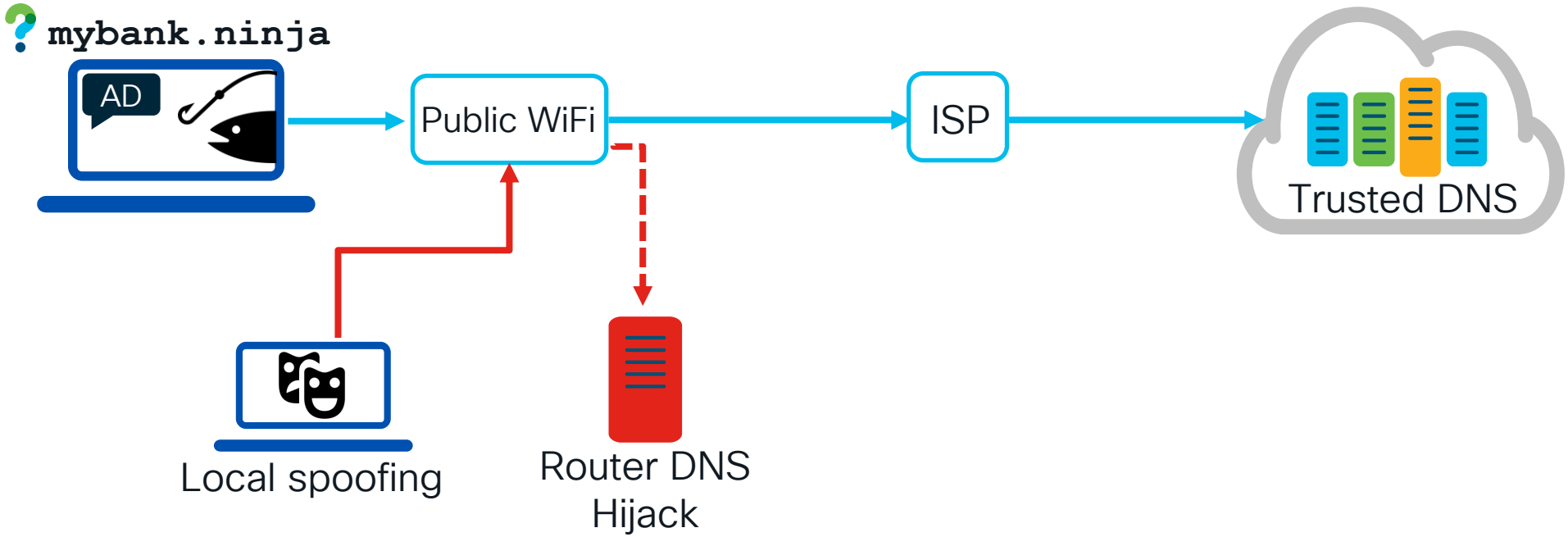
DNS attack ecosystem



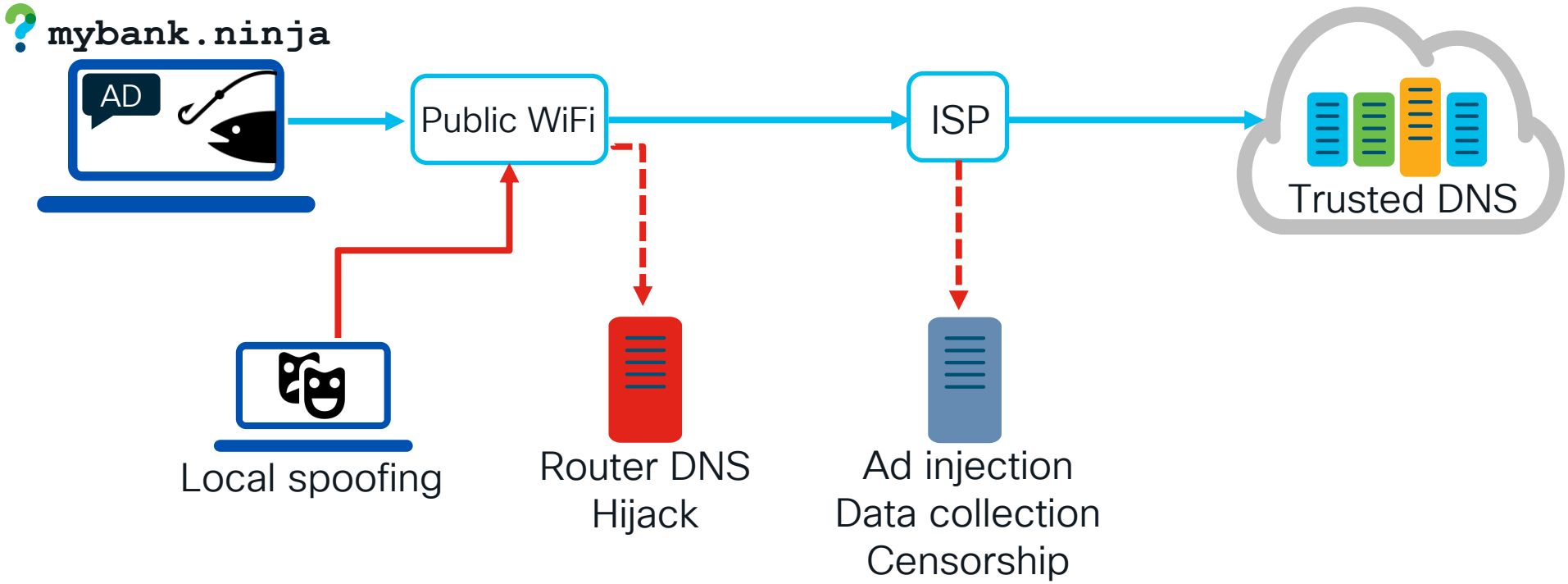
DNS attack ecosystem



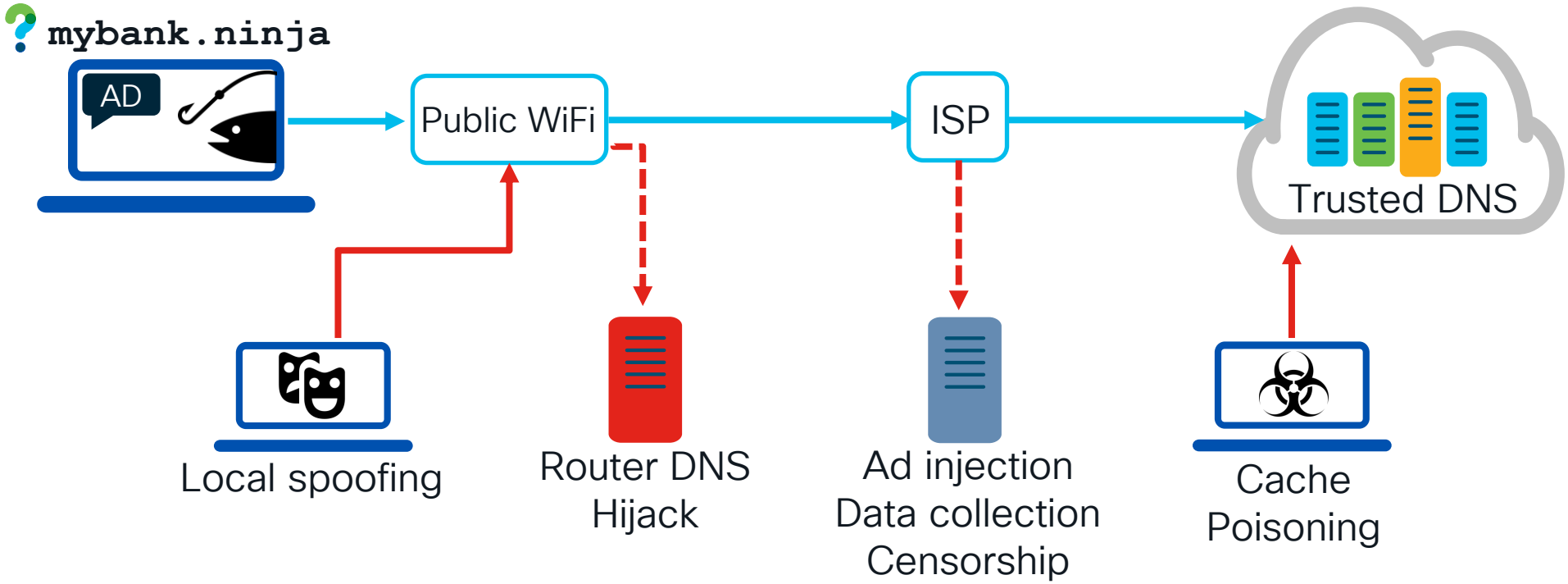
DNS attack ecosystem



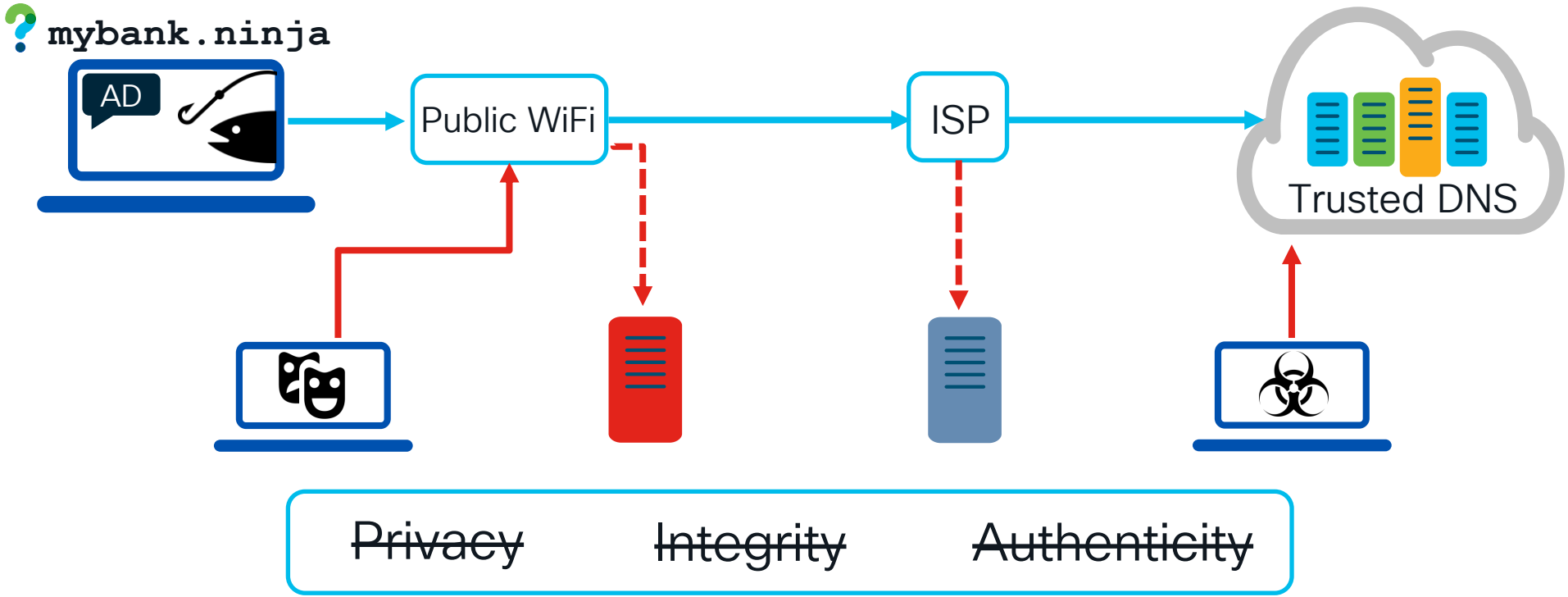
DNS attack ecosystem



DNS attack ecosystem



DNS attack ecosystem



DNSSEC and DNSCrypt

DNSSEC basics

New record types for crypto operations:

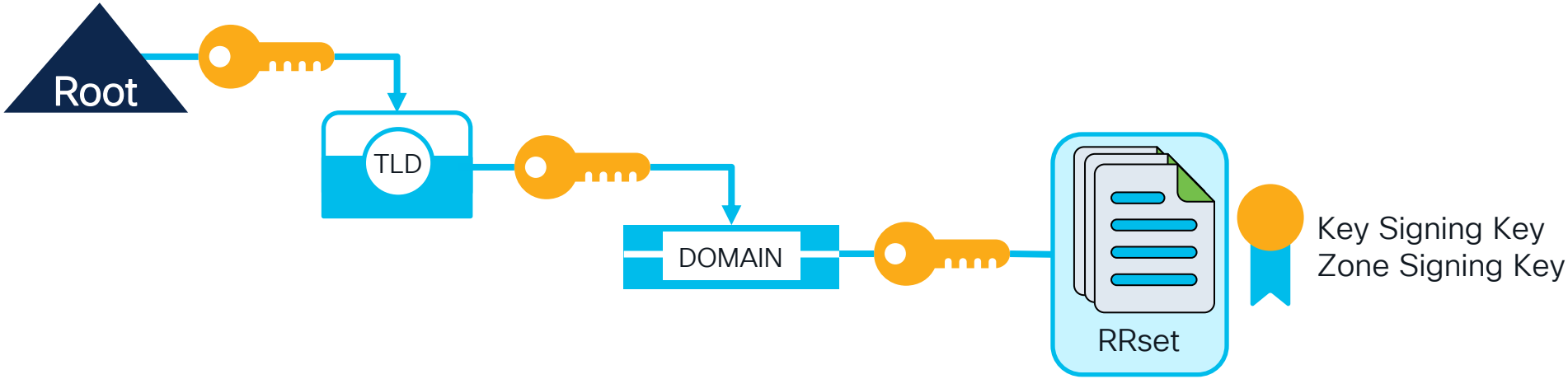
RRSIG: Crypto Signature

DS: Hash of Public Key

CDNSKEY/CDS: Updates to parent zones

DNSKEY: Public Key

NSEC/NSEC3: *Denial-of-Existence*



Early DNSSEC development
IETF Meeting in Houston, TX 1993

- The goals of DNSSEC were limited from the outset
  - Data disclosure considered out of scope
  - Backwards compatibility
  - No detailed threat model
  - The resulting requirements were:
    - *Data integrity*
    - *Data origin authentication*
- Root zone wasn't signed until 2010
  - Keys first rotated in 2018
  - This took eight phases over two years

Early DNSSEC development
IETF Meeting in Houston, TX 1993

- The goals of DNSSEC were limited from the outset
  - Data disclosure considered out of scope
  - Backwards compatibility
  - No detailed threat model
  - The resulting requirements were:
    - *Data integrity*
    - *Data origin authentication*
- Root zone wasn't signed until 2010
  - Keys first rotated in 2018
  - This took eight phases over two years

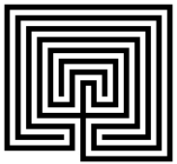
Trivia:

What browser was launched the same year (1993) and was the first to show images inline with text in the same window?

Early DNSSEC development
IETF Meeting in Houston, TX 1993

- The goals of DNSSEC were limited from the outset
  - Data disclosure considered out of scope
  - Backwards compatibility
  - No detailed threat model
  - The resulting requirements were:
    - *Data integrity*
    - *Data origin authentication*
- Root zone wasn't signed until 2010
  - Keys first rotated in 2018
  - This took eight phases over two years

DNSSEC weaknesses



Complexity

- Small config errors cause failure
- PKI and crypto knowledge
- Key rotation (Oct 2018)

Hierarchical

- Problems roll downhill
- Central point of failure

Denial of Service

- Responses are much larger
- Better for amplification

Privacy and Enumeration

- Doesn't address snooping
- NSEC creates new vuln

~~Privacy~~ Integrity Authenticity

NSEC3 vs. The White Lies Approach

NSEC3

- Provide the Next Secure (NSEC) record if name does not exist
- Can be used to enumerate zones
- NSEC3 hashes the names, in preserved alphabetical order, and allows for opt-out for child zones

White lies

- RFC 4470 / 4471 (April 2006)
- Make up the next lexical name on the fly and sign it
- More vulns!
  - Real-time access to private keys
  - More computationally expensive
  - Chosen-plaintext attacks

DNSCrypt

- OpenDNS announced the first public DNS server in 2011
- DNS requests/responses are unchanged
- Runs on UDP or TCP 443
- Enforces Public Key Pinning
- Pads packets to hide length
- Mitigates amplification attacks

Privacy Integrity Authenticity

DNSCrypt

- OpenDNS announced the first public DNS server in 2011
- DNS requests/responses are unchanged
- Runs on UDP or TCP 443
- Enforces Public Key Pinning
- Pads packets to hide length
- Mitigates amplification attacks

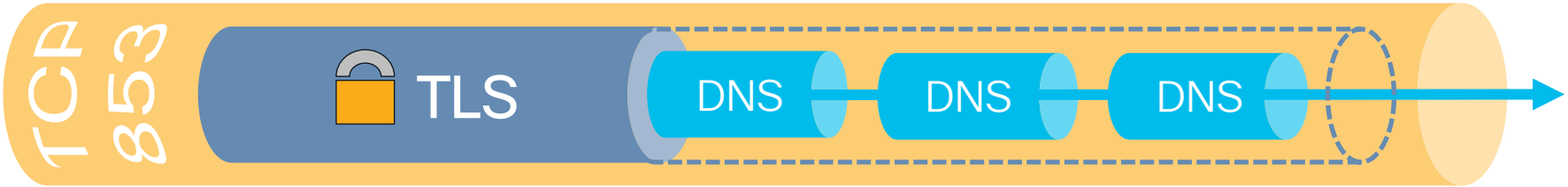
Privacy Integrity Authenticity

DNSCrypt

- Not a proposed IETF standard
- Fragmented implementations
- Always a third-party application
- No native OS support
- Complexity of deployment

DNS over TLS (DoT)

DoT overview



- Proposed IETF standard (RFC 7858)
- Defines a well-known port (TCP 853)
- Focuses on client-to-recursive server communication (stub resolvers)
- Connection re-use is encouraged, TCP Fast-Open and TLS session resumption are encouraged for performance
- Supported in Umbrella as of Jan 28, 2022

DoT modes

Opportunistic

- Analogous to SMTP opportunistic encryption
- Designed to aid in transition or for roaming clients
- Vulnerable to downgrade attack

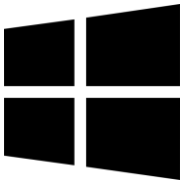
Strict

- Requires TLS and does not fall back
- Requires OOB key management
- Uses Simple Public Key Management (SPKI)

DoT OS adoption

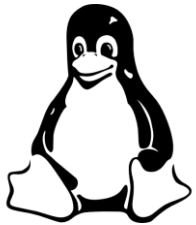
Android

- Supported in Pie
- Enabled by default
- Uses dns.google



Windows

- No native support
- Stubby or Knot-resolver



Linux

- Supported in system-resolved
- Add the DNSOverTLS option

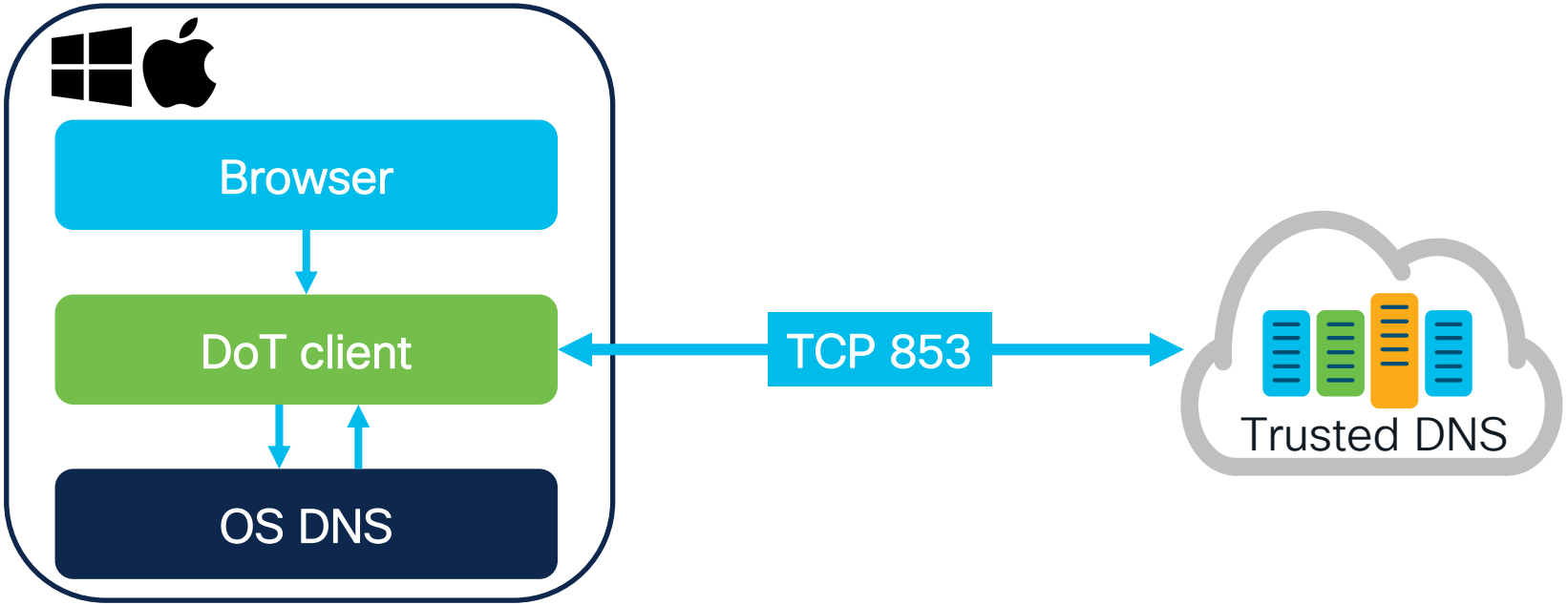
iOS

- iOS 14 native support
- macOS 11 native support
- Stubby or Knot-resolver

The middlebox problem / feature

Shimming DoT into the stack

https://dnsprivacy.org/wiki/display/DP/DNS+Privacy+Daemon+-+Stubby
https://www.knot-resolver.cz/



Supported recursive DoT resolvers

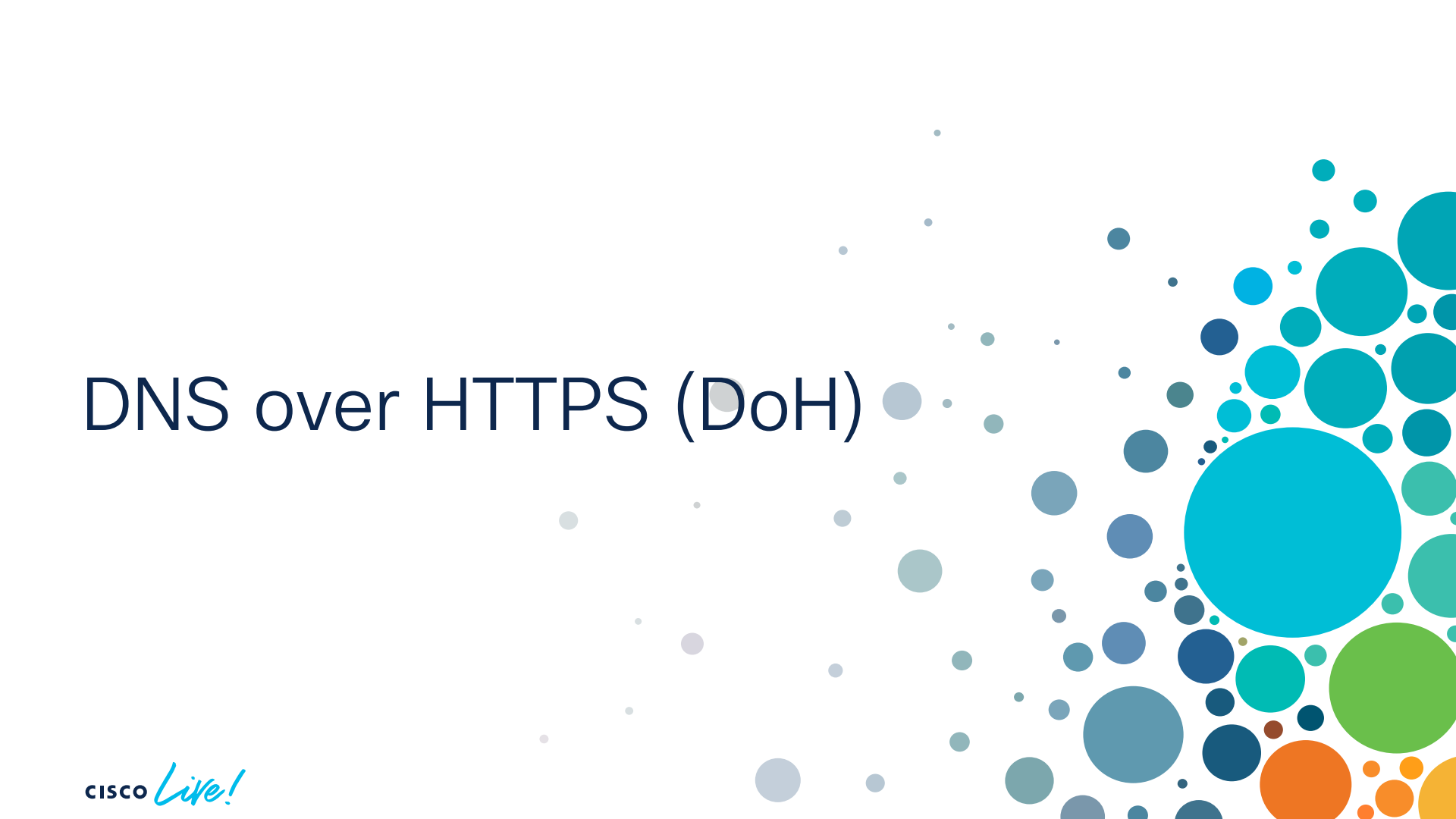
- https://dnsprivacy.org/wiki/display/DP/DNS+Privacy+Public+Resolvers

DNS-over-TLS (DoT)

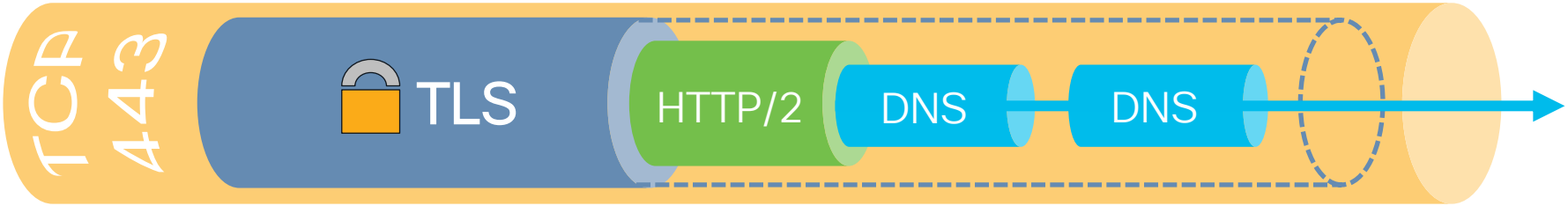
Details are provided in the Stubby config file for users who want to enable them.

Hosted by	IP addresses	TLS Ports	Hostname for TLS authentication	Base 64 encoded form of SPKI pin(s) for TLS authentication (RFC7858)	Notes
Quad9 'secure'	9.9.9.9 2620:fe::fe	853	dns.quad9.net	**Quad9 do NOT publish or recommend use of SPKI pins with their servers.**	See https://quad9.net and their FAQ for details of privacy, logging and filtering policies on the main and alternative addresses(1). UDP and TCP service are also available on these addresses.
Quad9 'insecure'	9.9.9.10 2620:fe::10	853	dns.quad9.net		
Cloudflare	1.1.1.1 or 1.0.0.1 2606:4700:4700::1111 or 2606:4700:4700::1001	853	cloudflare-dns.com	**Cloudflare do NOT publish or recommend use of SPKI pins with their servers.**	https://blog.cloudflare.com/announcing-1111/ https://blog.cloudflare.com/dns-resolver-1-1-1-1/ PRIVACY POLICY: https://developers.cloudflare.com/1.1.1.1/commitment-to-privacy/privacy-policy/privacy-policy/

DNS over HTTPS (DoH)



DoH overview



- Proposed IETF standard (RFC 8484)
- Runs over HTTPS (TCP 443)
- Focuses on client-to-recursive server communication (stub resolvers)

- HTTP/2 provides reordering, parallelism, priority, and header compression for performance
- IANA registered Media Type
  - `application/dns-message`

Query methods
GET

- GET method encodes the query in Base64url
- “Friendlier” to many HTTP cache implementations

```
:method = GET
:scheme = https
:authority = dnsserver.example.net
:path = /dns-query?dns=AAABAAABAAAAAAAAA3d3dwdl…
accept = application/dns-message
```

Query methods
POST

- POST method encodes the query in the message body
- Content-Type header indicates that it is a DNS query

```
:method = POST
:scheme = https
:authority = dnsserver.example.net
:path = /dns-query
accept = application/dns-message
content-type = application/dns-message
content-length = 33

<33 bytes represented by the following hex encoding>

00 00 01 00 00 01 00 00 00 00 00 00 03 77 77 77 07 65 78 61 6d 70 6c 65 03
63 6f 6d 00 00 01 00 01
```

Response

```
response: {
      "Status": 0,
      "TC": false,
      "RD": true,
      "RA": true,
      "AD": true,
      "CD": false,
      "Question": [{
                  "name": "example.com.",
                  "type": 28
            }
      ],
      "Answer": [{
                  "name": "example.com.",
                  "type": 28,
                  "TTL": 1005,
                  "data": "2606:2800:220:1:248:1893:25c8:1946"
            }
       ]
 }
```

*https://wiki.mozilla.org/Trusted_Recursive_Resolver

Firefox implementation

- `network.trr.bootstrapAddress`
  - Sets the initial resolver to use to find the DoH server IP address
  - Blank by default (uses system resolver)
- `network.trr.uri`
  - The address of the DoH server to be used
  - Default is https://mozilla.cloudflare-dns.com/dns-query if DoH is enabled
- `network.trr.mode`

  0 - Off (default). use standard native resolving only (don't use TRR at all)

  1 - Reserved (used to be Race mode)

  2 - First. Use TRR first, and only if the name resolve fails use the native resolver as a fallback.

  3 - Only. Only use TRR. Never use the native resolver

  4 - Reserved (used to be Shadow mode)

  5 - Off by choice. This is the same as 0 but marks it as done by choice and not done by default.

Firefox implementation

https://github.com/mozilla/policy-templates#dnsoverhttps

DNSOverHTTPS

Configure DNS over HTTPS.

`Enabled` determines whether DNS over HTTPS is enabled

`ProviderURL` is a URL to another provider.

`Locked` prevents the user from changing DNS over HTTPS preferences.

`ExcludedDomains` excludes domains from DNS over HTTPS.

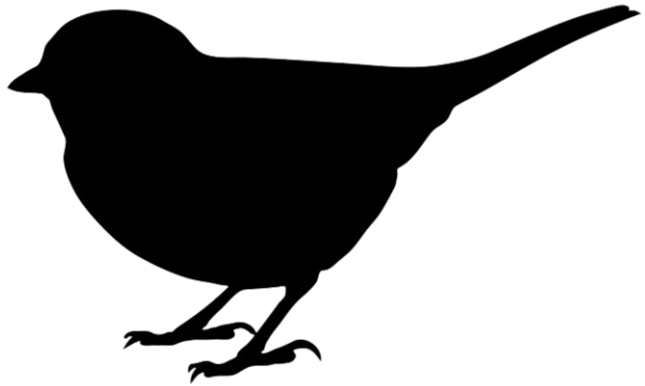
Compatibility: Firefox 63, Firefox ESR 68 (ExcludedDomains added in 75/68.7)
CCK2 Equivalent: N/A
Preferences Affected: `network.trr.mode`, `network.trr.uri`

Firefox implementation

Canary domain

- Firefox will attempt to resolve the domain using the system resolver
- NOERROR with a host record (A or AAAA) will result in DoH being enabled

use-application-dns.net



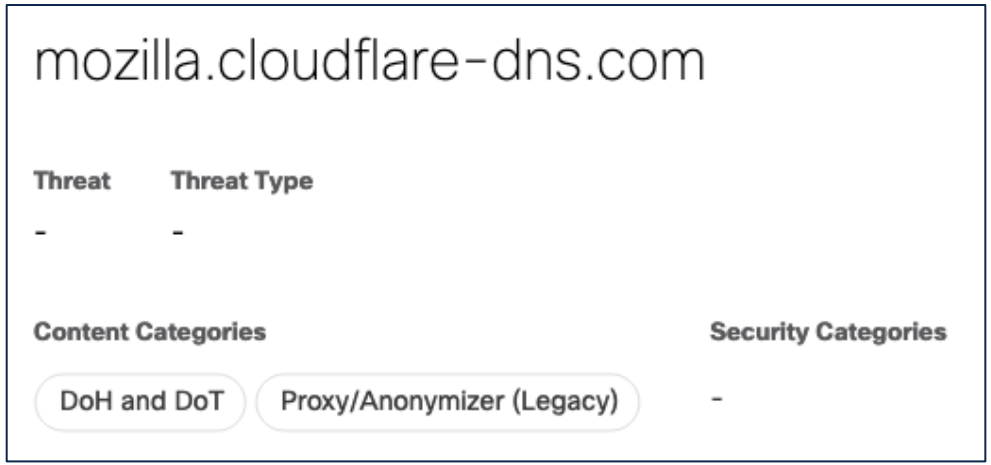
PowerShell command to add the domain:

```
Add-DnsServerQueryResolutionPolicy `
    -Name "CanaryDomainPolicy" `
    -Action DENY `
    -FQDN "EQ, use-application-dns.net"
```

Umbrella blocking DoH resolvers

https://support.umbrella.com/hc/en-us/articles/360001371526-Firefox-and-DNS-over-HTTPS-default

- Umbrella has a dedicated DoH and DoT category
  - Previously Proxy/Anonymizer
- For IP-based configuration, use Cloud Firewall



Chrome implementation

https://www.chromium.org/developers/dns-over-https

- Chrome has a local table which maps DoH servers to their non-DoH equivalent
- If the system resolver supports DoH, then Chrome will take over DNS (using DoH)
- Enabled by default in v83
- The currently mapped providers:
  - https://source.chromium.org/chromium/chromium/src/+/HEAD:net/dns/public/doh_provider_entry.cc

The challenges to business and privacy

- No way to define internal domains
  - Breaks internal resolution and split-DNS
- Bypasses system DNS
  - Internal DNS controls are now useless
- Can only be identified using the SNI and destination IP address
  - Whack-a-mole for firewall administrators
- Concentrates DNS to a handful of providers
  - Privacy and tracking is again a concern…

"DoH is an over the top bypass of enterprise and other private networks. But DNS is part of the control plane, and network operators must be able to monitor and filter it. Use DoT, never DoH."

Paul Vixie, 2018

DoH in malicious activity

- Many C2 proofs-of-concepts are publicly available
- Godlua backdoor discovered using DoH for C2 in April 2019

First-ever malware strain spotted abusing new DoH (DNS over HTTPS) protocol

Godlua, a Linux DDoS bot, is the first-ever malware strain seen using DoH to hide its DNS traffic.

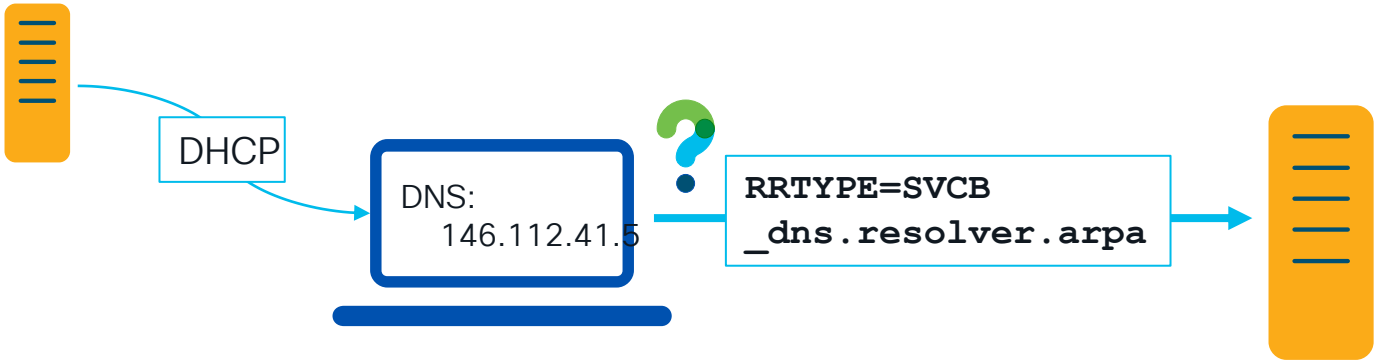
https://blog.netlab.360.com/an-analysis-of-godlua-backdoor-en/

Methods for detection and control

- Block TCP 853 outbound (DoT)
- Configure the Firefox canary domain and use GPO to disable it
- Configure Firefox to log all DNS queries (including DoH):
  - `setx MOZ_LOG timestamp,rotate:200,nsHostResolver:4`
  - `setx MOZ_LOG_FILE C:\Logs\%USERNAME%-Firefox-DNS-log.txt`
- Monitor and block the published DoT and DoH IP addresses
  - Until they are shared with major services…
- Implement decrypting proxies

Discovery of Designated Resolvers (DDR)

https://www.ietf.org/archive/id/draft-ietf-add-ddr-01.html



Hosts can use the SVCB (type64) DNS record to find out what encrypted DNS is available from their assigned DNS resolver

Discovery of Designated Resolvers (DDR)

https://www.ietf.org/archive/id/draft-ietf-add-ddr-01.html

```
_dns.resolver.arpa: type SVCB, class IN
    Name: _dns.resolver.arpa
    Type: SVCB (General Purpose Service Endpoints) (64)
    Class: IN (0x0001)
    Time to live: 300 (5 minutes)
    Data length: 81
    SvcPriority: 5
    TargetName: dns.opendns.com
    SvcParam: alpn=dot
    SvcParam: port=853
    SvcParam: ipv4hint=208.67.220.220,208.6
    SvcParam: ipv6hint=2620:119:35::35,2620
```

DoT Endpoint

DoH Endpoint

```
_dns.resolver.arpa: type SVCB, class IN
    Name: _dns.resolver.arpa
    Type: SVCB (General Purpose Service Endpoints) (64)
    Class: IN (0x0001)
    Time to live: 300 (5 minutes)
    Data length: 94
    SvcPriority: 10
    TargetName: dns.opendns.com
    SvcParam: alpn=h2
    SvcParam: ipv4hint=208.67.220.220,208.67.222.222
    SvcParam: ipv6hint=2620:119:35::35,2620:119:53::53
    SvcParam: key7=/dns-query{?dns}
```

Discovery of Designated Resolvers (DDR)

https://www.ietf.org/archive/id/draft-ietf-add-ddr-01.html

- Umbrella was the first to implement
  - Partnered with MS and Quad9
- Supported in newer Windows builds
  - Windows 11
  - Server 2022

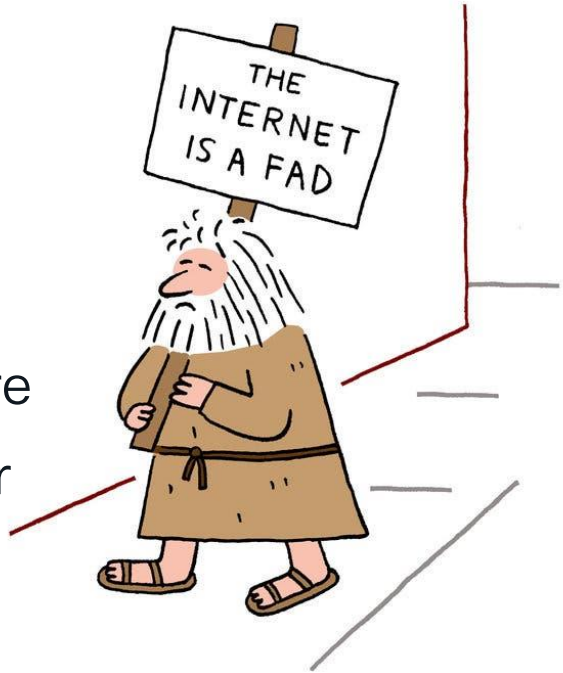
- https://blogs.cisco.com/security/cisco-interop-discovery-of-designated-resolvers-protocol-implemented
- https://umbrella.cisco.com/blog/enhancing-support-dns-encryption-with-dns-over-https
- https://techcommunity.microsoft.com/t5/networking-blog/making-doh-discoverable-introducing-ddr/ba-p/2887289

iOS behavior changes (Sept 2020)

- iOS 14 and MacOS 11
  - Users-set DoH resolver can override DHCP or RA
  - Domains-set DoH resolvers can override DHCP or RA
  - App-set DoH resolver can override the DNS resolver set by DHCP or RA
- Does not affect Apple's DNS Proxy
  - Cisco Security Connector
  - MacOS Umbrella Roaming Client
  - AnyConnect Roaming Security

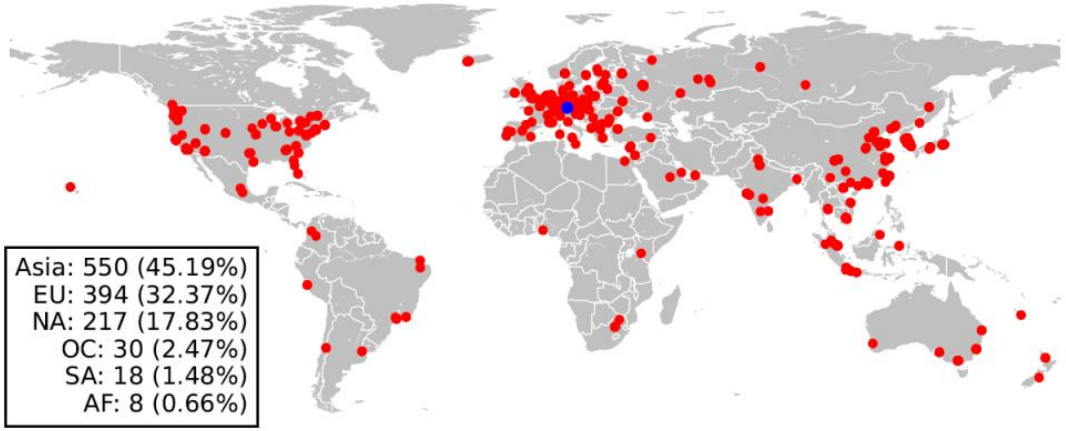
Takeaways

- Encrypted DNS is already on your network
- Understand the implications
- Block and monitor where relevant
- Be mindful of who your chosen providers are
- If you think this transition is fun...just wait for encrypted SNI and QUIC!



DNS over QUIC

- Currently in draft status
  - https://datatracker.ietf.org/doc/draft-ietf-dprive-dnsoquic/
  - Ports proposed:
    - UDP 784
    - UDP 853
    - UDP 8853
  - Research shows fast adoption and performance
- AdGuard and NextDNS already use it in production



https://blog.apnic.net/2022/03/29/a-first-look-at-dns-over-quic/

Technical session surveys

- Attendees who fill out a minimum of four session surveys and the overall event survey will get Cisco Live branded socks!
- Attendees will also earn 100 points in the Cisco Live Game for every survey completed.
- These points help you get on the leaderboard and increase your chances of winning daily and grand prizes.

Security reference architecture

CISCO SECURE

TALOS — Threat Intelligence | Malware Analytics | Actionable Intelligence | Unmatched Visibility | Collective Responses

Security Operations

SECURE X (XDR)

- Managed Detection and Response Services
- Security, Orchestration, Automation and Response
- Incident Response and Remediation Services
- Threat Visibility & Hunting
- Device Insights
- Kenna Vuln Mgmt
- Secure Cloud Insights
- 3rd Party Integrations

User/Device Security

ZERO TRUST

Adaptive MFA | Passwordless | Trust

Duo Secure Access

Secure E-mail

SASE/REMOTE WORKER

Unified Client | EDR | Cloud Managed

Cisco Secure Client

- VPN
- Posture
- Telemetry
- Threat
- Query

ThousandEyes (Visibility)

Device Mgmt: Meraki SM OS, App Control

Network Security

Cloud Edge

SECURE ACCESS SERVICE EDGE (SASE) | ZERO TRUST

Threat Protection | Secure Access Control | Managed Remote Access

PRIVATE CLOUD EDGE (MSP or CUSTOMER)

Reliable | Scalable | Flexible

Umbrella/Duo

- ZTNA
- DNS-layer security
- Secure web gateway
- L7 firewall + IPS
- Cloud access security broker/ shadow IT
- RAaaS
- SSL decryption
- Remote browser Isolation
- Data loss prevention
- Cloud malware detection

SDWAN

- Meraki SDWAN
- SDWAN by Viptela
- Secure Firewall
- ThousandEyes
- Cloud DDoS,WAF

On-Premises

SASE/SDWAN

Scalable | Flexible | Visibility | Comprehensive Security

Network Edge

- Meraki SDWAN
- SDWAN by Viptela
- Secure Firewall
- ThousandEyes

IoT/OT SECURITY

Secure Critical Infrastructure | Unified IT and OT

- Industrial Router
- Industrial Firewall
- Industrial Switch/AP
- Cyber Vision
- ISE TrustSec

ZERO TRUST

Segmentation | Identity and Context | Profiling | Containment | Encrypted Visibility

- Security Analytics and Logging
- Secure Firewall
- DuoCloud SSO+IDP
- Network Gateway
- Secure DDoS
- Meraki Full Stack
- Secure Network Analytics
- Secure Web Appliance
- ISE TrustSec
- Cisco DNA Center

Application Security

ZERO TRUST

Policy | API Security
Application Segmentation
Run-time Application Security

Application Security Stack

- Cloud Native Security
- APIC
- Secure Workload
- Secure Application by AppDynamics

App Observability | Detection | Response

- Hybrid Private
- Public Cloud
- Secure Cloud Analytics
- Secure Firewall
- ThousandEyes
- Secure DDoS, WAF/Bot

Cisco learning and certifications

From technology training and team development to Cisco certifications and learning plans, let us help you empower your business and career. www.cisco.com/go/certs

Pay for Learning with Cisco Learning Credits

(CLCs) are prepaid training vouchers redeemed directly with Cisco.

Learn

Cisco U.
IT learning hub that guides teams and learners toward their goals

Cisco Digital Learning
Subscription-based product, technology, and certification training

Cisco Modeling Labs
Network simulation platform for design, testing, and troubleshooting

Cisco Learning Network
Resource community portal for certifications and learning

Train

Cisco Training Bootcamps
Intensive team & individual automation and technology training programs

Cisco Learning Partner Program
Authorized training partners supporting Cisco technology and career certifications

Cisco Instructor-led and Virtual Instructor-led training
Accelerated curriculum of product, technology, and certification courses

Certify

Cisco Certifications and Specialist Certifications
Award-winning certification program empowers students and IT Professionals to advance their technical careers

Cisco Guided Study Groups
180-day certification prep program with learning and support

Cisco Continuing Education Program
Recertification training options for Cisco certified individuals

Here at the event? Visit us at **The Learning and Certifications lounge at the World of Solutions**

Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

cisco Live!

Thank you


cisco Live!
ALL IN