Announcement

- Take-home Exam 1 is due 3 March, 2023

- Mid-term survey
  - Available in Quiz section
  - Anonymous.
  - Optional, but your feedback is greatly appreciated!

- Quiz 3
  - Opens at 9am on 28 Feb, 2023
  - Closes at 6:30pm on 6 March 2023
  - Covers Week 5 and 6 lecture slides

CS5321 Network Security
Week 7: DNS Security

Daisuke MASHIMA

http://www.mashima.us/daisuke/index.html

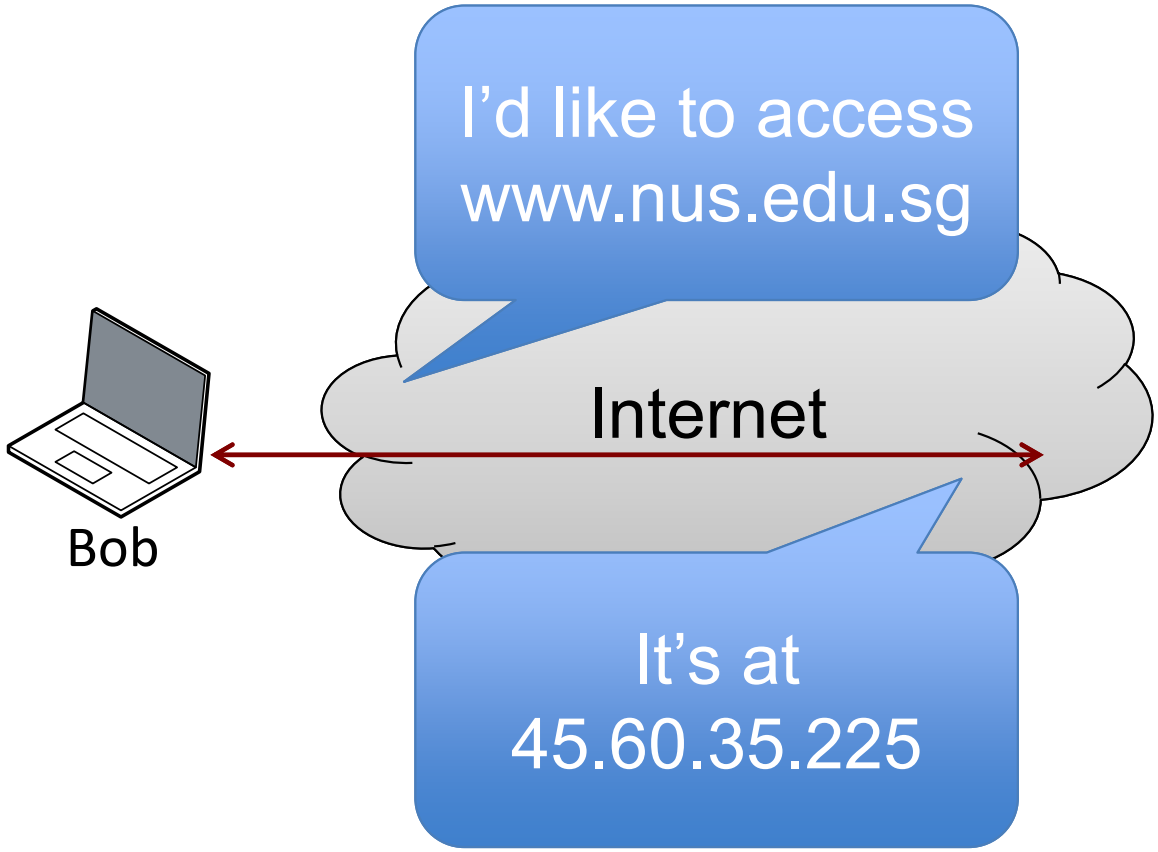
2022/23 Sem 2

Agenda

- DNS overview
- Integrity of DNS
  - DNSSEC
- Confidentiality of DNS
  - DNS over Encryption

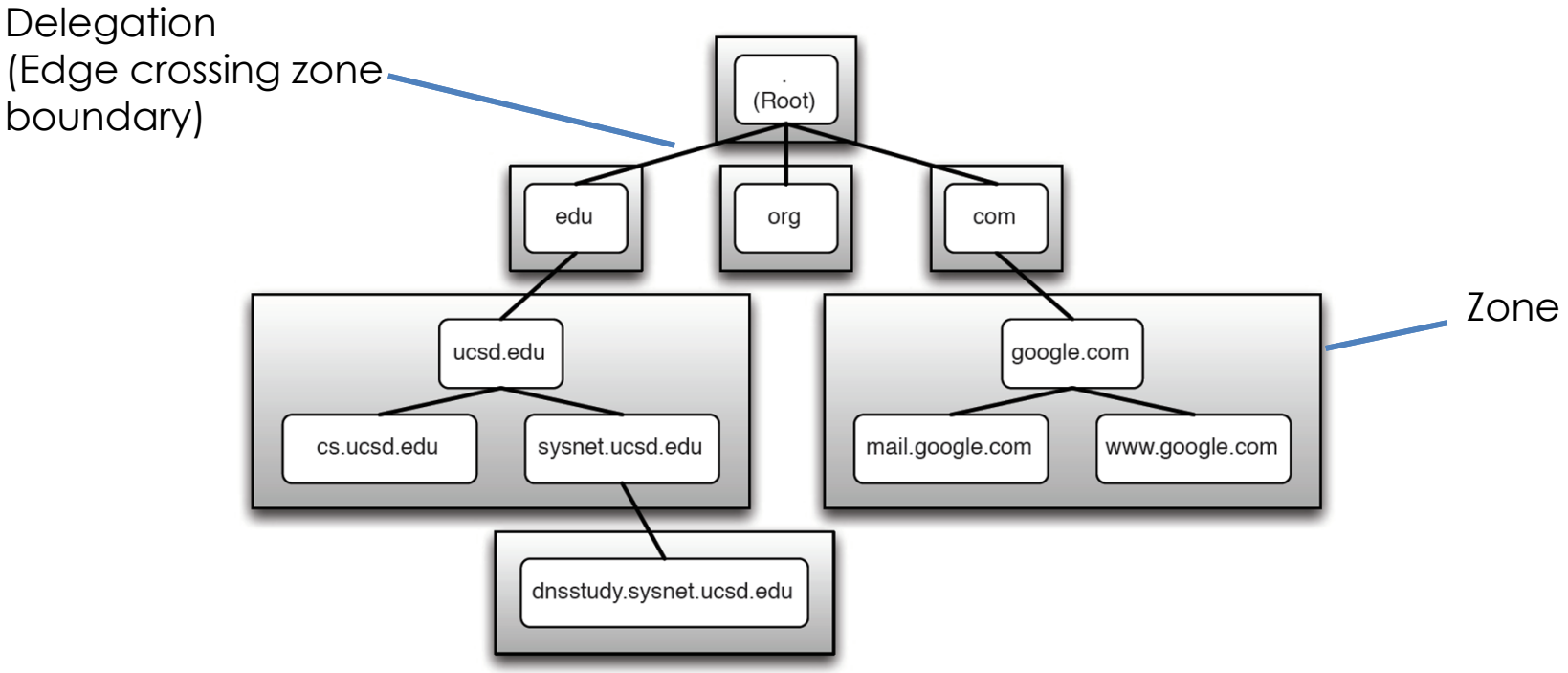
The "*bootstrapping*" protocol of the Internet

- Translate human-readable addresses to IP addresses
- Often the very first network service

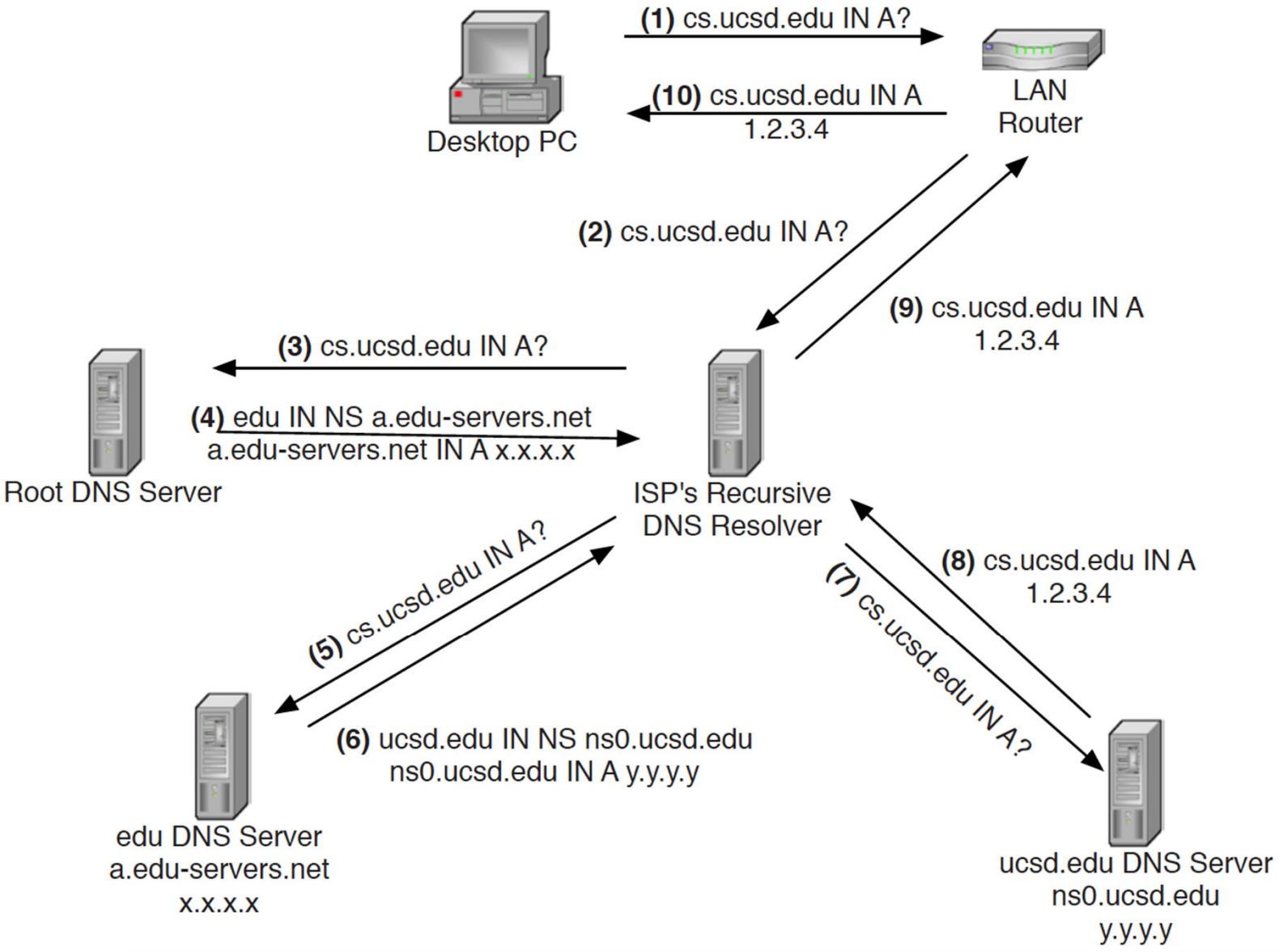


DNS Name Tree

- DNS name is dot-separated concatenation of ***labels*** ***(e.g., "cs", "ucsd", "edu").***
- DNS namespace is organized as a tree whose nodes are labels.
- DNS is a ***distributed system.*** (no central entity maintaining a DB for all names)
- Namespace is broken up into **"zones"**, which are administrative spaces managed by different organizations
  - Each zone has **authoritative name server(s)**
- Authority over a subtree can be **delegated**. Delegation defines zone boundaries.



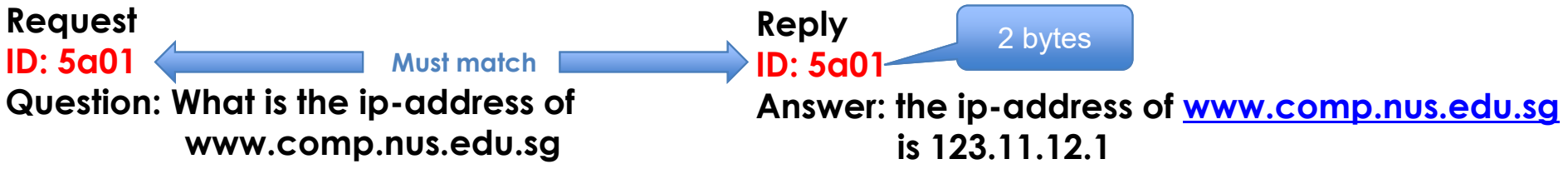
DNS Name Resolution



DNS Messages

Header (12 bytes)	Contains fields that describe the type of message and provide important information about it (e.g., ID). Also contains fields that indicate the number of entries in the other sections of the message.
Question	Carries one or more "questions", that is, queries for information being sent to a DNS name server.
Answer	Carries one or more resource records that answer the question(s) indicated in the *Question* section above.
Authority	Contains one or more resource records that point to authoritative name servers that can be used to continue the resolution process.
Additional	Conveys one or more resource records that contain additional information related to the query that is not strictly necessary to answer the queries (questions) in the message.

Above table from http://www.tcpipguide.com/free/t_DNSMessageProcessingandGeneralMessageFormat.htm



Top security threats to DNS

- Availability
  - Distributed denial-of-service (DDoS)
- Integrity
  - Malicious open recursive resolvers
  - Network man-in-the-middle attackers
  - Cache poisoning attacks
- Confidentiality
  - Pervasive monitoring
  - Censorship

scope of this lecture

Defence against DDoS

- Examples
  - DDoS attack against StarHub DNS server (2016)

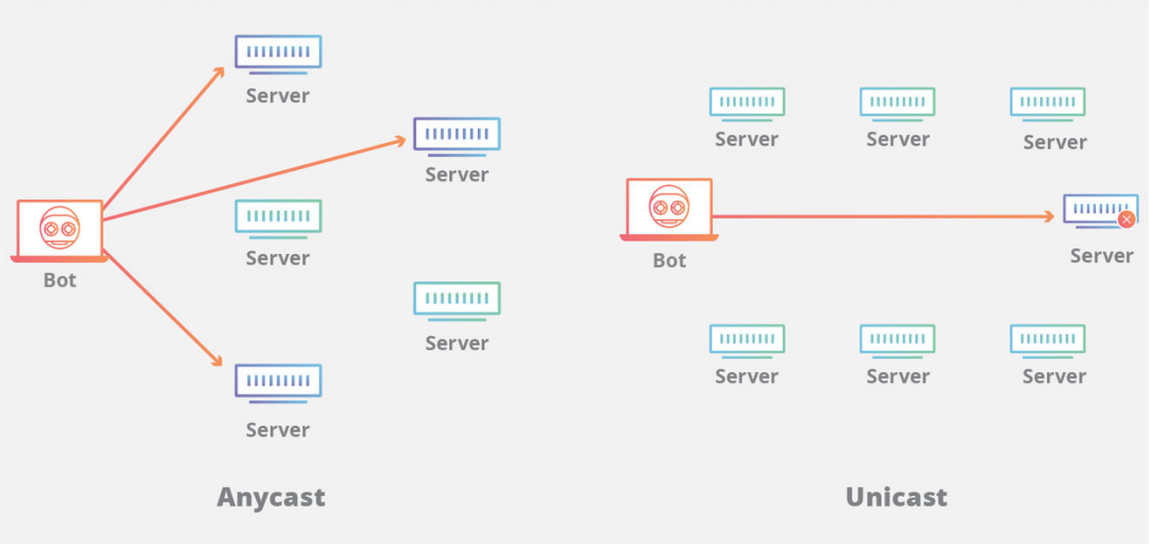
SINGAPORE TELECOMS GROUP STARHUB HIT BY ATTACKS ON DNS SERVERS

Less than a week after the attack on US-based DNS service Dyn, affecting websites and services from organisations including Amazon, Spotify, Twitter and Netflix to name just a few, it appears no random coincidence that a DDoS attack was responsible for disruption of services to Starhub's home broadband customers.

StarHub issued a statement on Tuesday (Oct 25) night to confirm that its broadband disruption on Saturday and Monday were due to "malicious distributed denial-of-service (DDoS) attacks on our Domain Name Servers (DNS)".

Defence against DDoS

- Overprovisioning
- Anycast (multiple servers with the same IP)
  - Used for root DNS
  - Typically implemented by using BGP
  - The same IP prefix is announced from multiple geographic locations
  - Each node utilizes route to the nearest server.



https://www.cloudflare.com/learning/dns/what-is-anycast-dns/

INTEGRITY OF DNS

Attack1: Poisoning a DNS Server's Cache

A bad guy controls a name server, `ns.hacker.com`. He also controls a machine with ip address **123.123.123.123**. The bad guy wants to pretend to be **`www.dbs.com.sg`**

1) The user is tricked to visit a website `badguy.hacker.com`. The Home PC needs to lookup its ip address. A request is sent to the name server `ns.myisp.com.`

2) The name server `ns.myisp.com` doesn't know the ip address. So it ask the name server `ns.hacker.com`

3) The malicious ns.hacker.com replies:

   " I don't know the address of **`badguy.hacker.com`**. *I would like to delegate* **`hacker.com`** *to the server* **`www.dbs.com.sg`**. *The ip address of* **`www.dbs.com.sg`** *is* **123.123.123.123**"

Now, the resolution fails and the Home PC can't get the ip address of `badguy.hacker.com`. An error message appears.

Attack 1: Poisoning a DNS Server's Cache

4) Later, the user wants to visit **www.dbs.com.sg** to perform some online banking transactions.

5) The name server `ns.myisp.com` is already poisoned. It gives the answer of 123.123.123.123, which is a server controlled by the hacker.

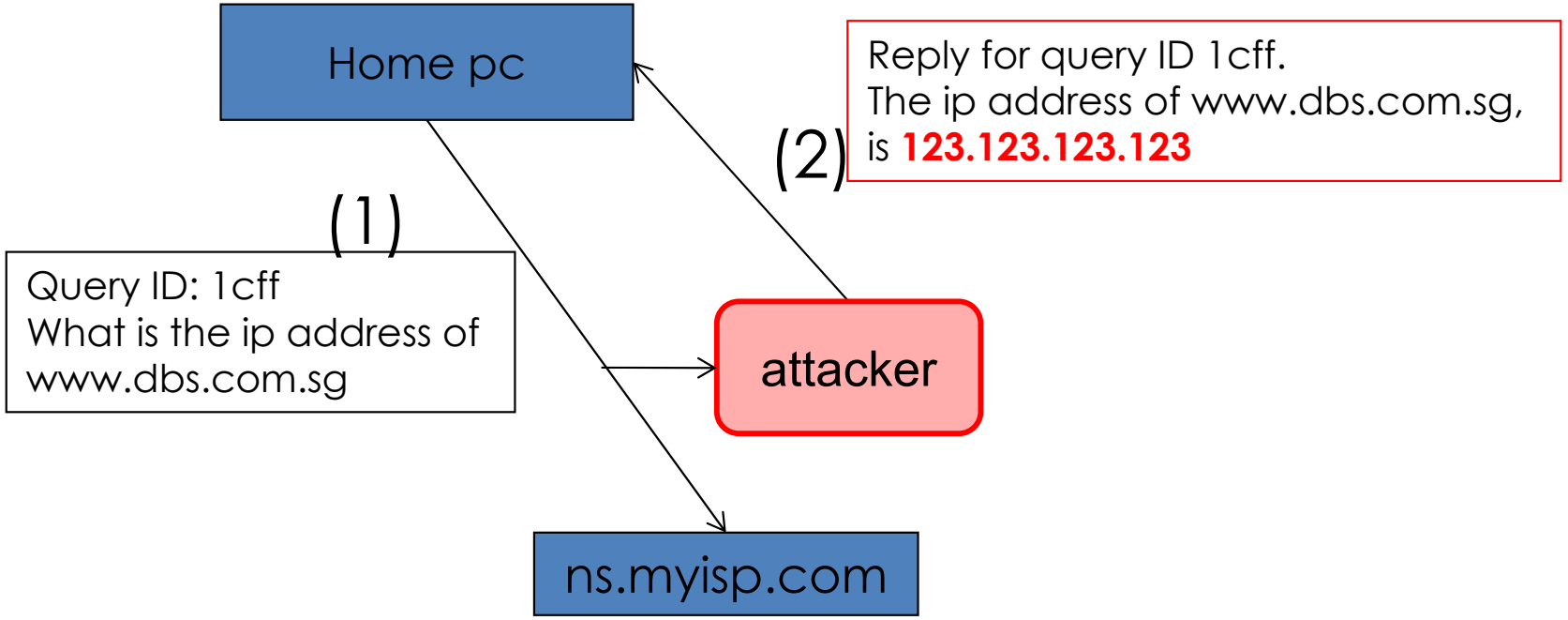
6) The user visits 123.123.123.123 to perform online banking transactions!

This attack was effective in the early days (before 1993, when BIND adopted **bailiwick rule.**)

- Bailiwick rule prevents malicious authoritative servers from providing DNS mappings for domains outside of their authority.

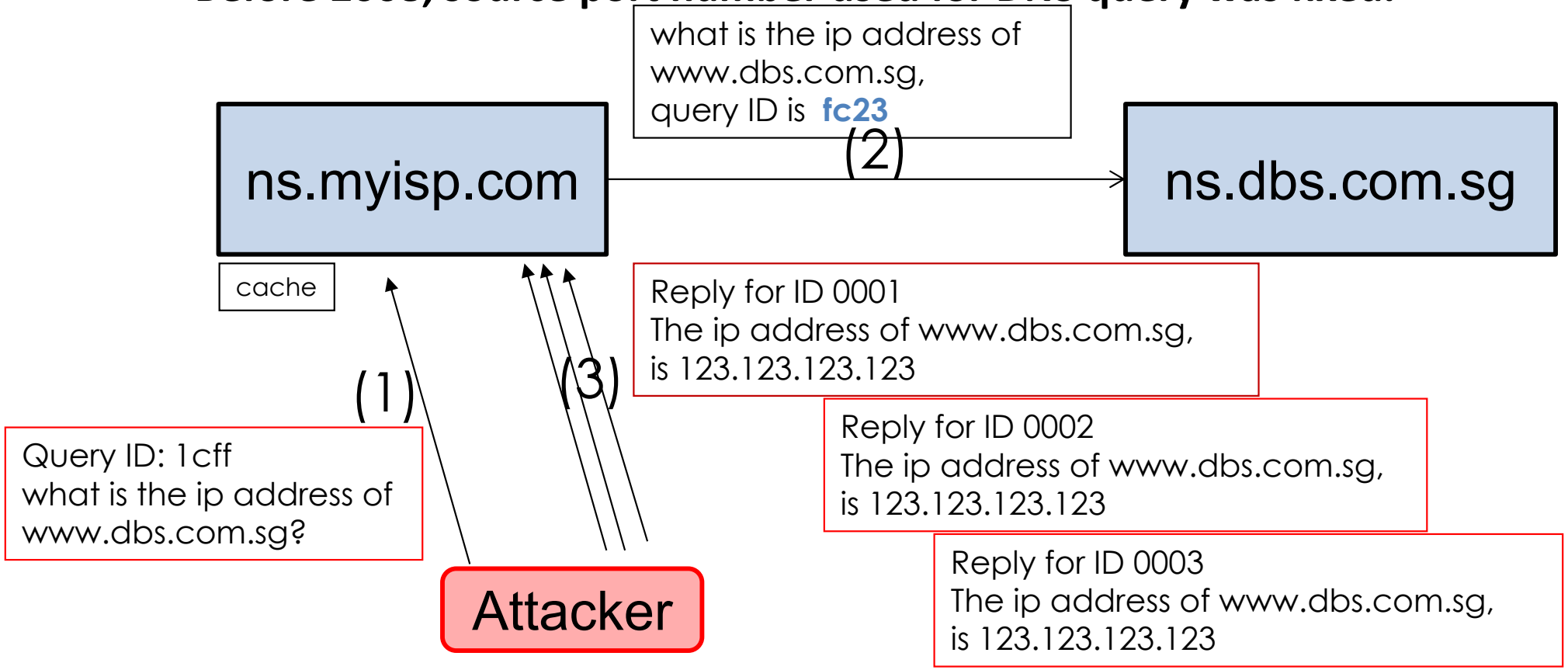
Attack 2: Sniffing and Spoofing

- A resolver (who could be a DNS server) sends a query to a DNS server. The message is intercepted by an attacker. The attacker composes a reply and sends it back to the client.
- In some settings, the attacker may intercept and drop the DNS request, so that ns.myisp.com will not receive the request.
- In other settings, the attack can only sniff but not drop the request. So the DNS request will reach ns.myisp.com. Hence , for the attack to be successful, the spoofed reply has to arrive before the authentic reply.



Attack 3: Flooding with spoofed replies

- In this attack, the adversary is **unable to sniffed the query**. So, he does not know the ID and thus can't compose the reply.
- A straightforward method is to flood the resolver with many replies.
  - Recall that a DNS request has an ID. The reply from the server must contains the same ID. The ID is **2 bytes (16 bits)**.
  - **Before 2008, source port number used for DNS query was fixed.**



Attack 3': Improvement of Attack 3

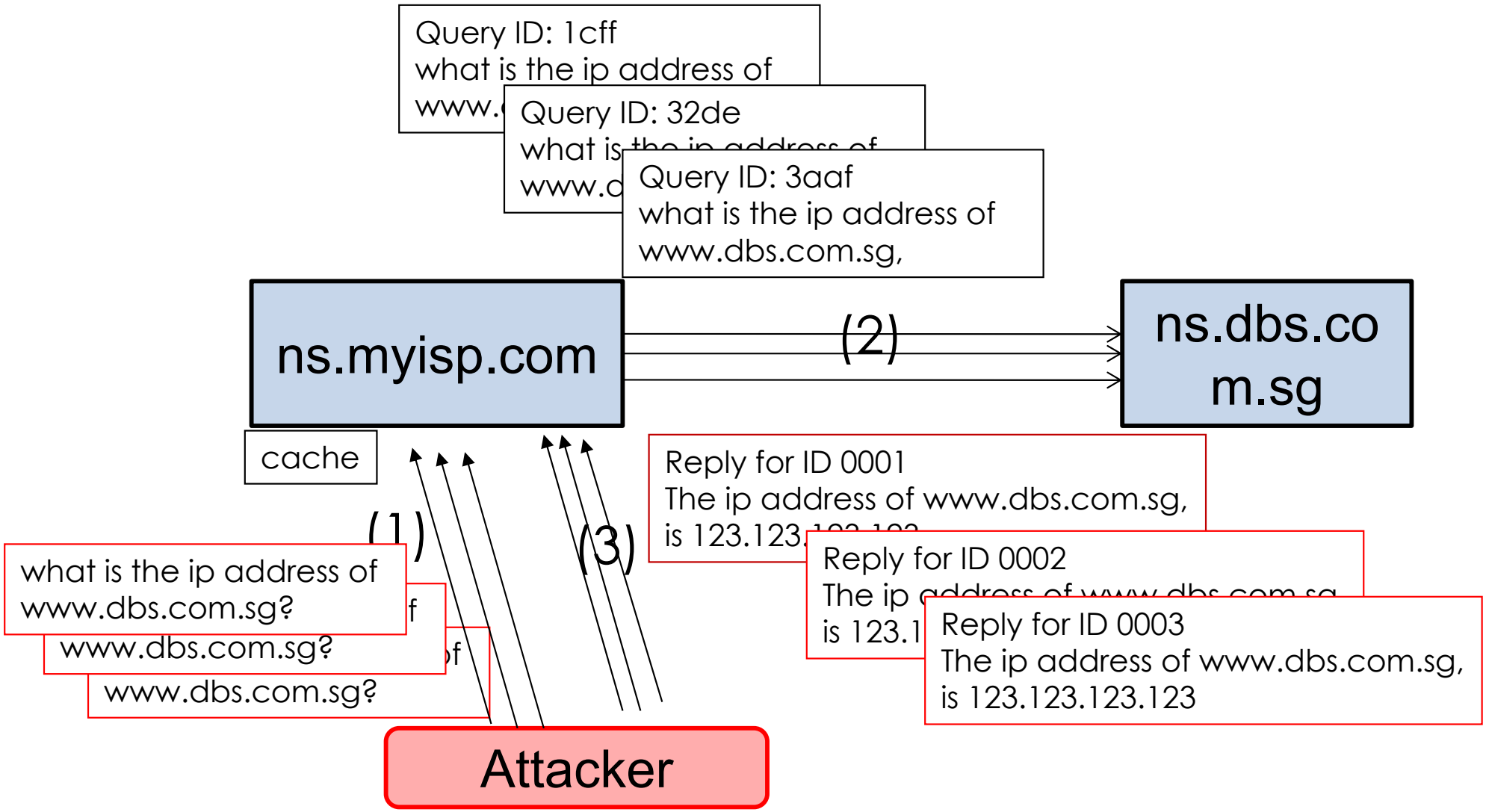
Since the ID has 2 bytes, so if the attacker manages to send 256 replies, the chance that it successfully poisons ns.myisp.com is only 256/65536 = **1/256**.

There was a flaw in the BIND software and it generated multiple queries for the same domain name at the same time.

Essentially, the attacker carry out these two steps:

1. Tricks the name server to send out multiple queries.
2. Spoofs and floods the name server, where the IDs are randomly generated.

Attack 3': Improvement of Attack 3



But once valid IP address is cached, an attacker needs to wait until the cache expires!

Attack 4: Kaminsky attack (Black Hat 2008)

- Consider the similar attacker model as the previous slide
- Query for subdomains: e.g., xyx12.google.com
- Fake Response:

- Advantage:
  - Attacker can try poisoning virtually infinitely because she can always find not-yet-cached subdomain!
  - Can introduce false mapping for authoritative server.

- Fix after 2008
  - UDP port number (16 bit) is randomized
  - Making the attack harder

DNSSEC

- DNSSEC (DNS Security Extensions) is a backward compatible security extension. It provides

  (1) data Integrity,

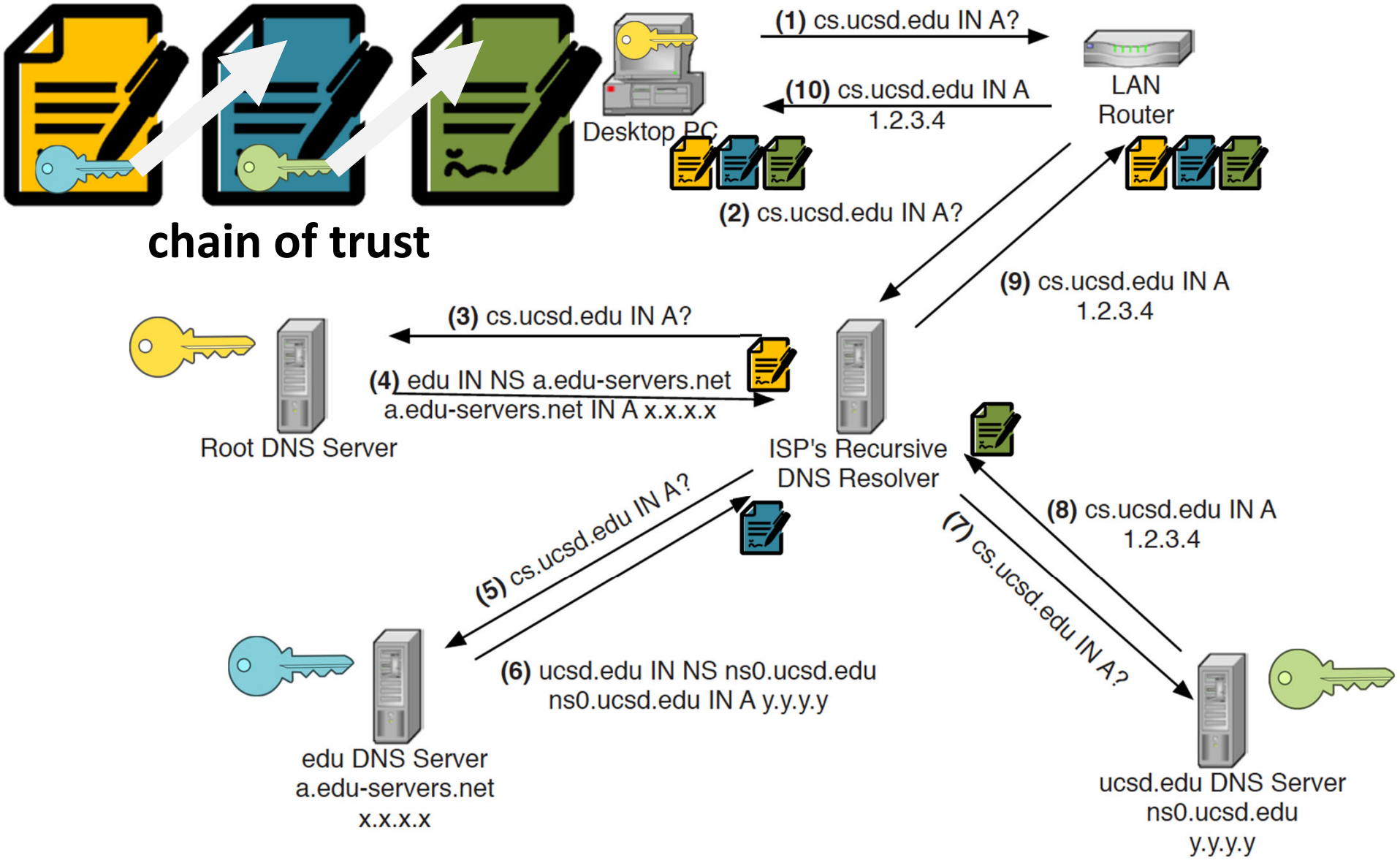
  (2) origin authenticity,

  (3) "authenticated denial of existence" – able to convince a resolver that a record does not exists.

  Note that confidentiality is not provided.

  Essentially, **the DNS server will sign (using PKI) the replies** so that a DNS resolver can verifies that the replies are indeed from the correct DNS server.

DNSSEC to the rescue



Technical Difficulties of DNSSEC

- Efficiency
  - It is very expensive to sign the response for every request. Note that public-key crypto is involved.
  - DNSSEC uses **pre-signed responses**. That is, the name server singed the messages for each valid domain names in its domain.
- Denial of Existence
  - The server has to give authenticated response even if the record is not found. It is not possible to pre-sign "not-found" response for all domain names that are not in the zone.
  - Pre-signing **groups of records that are not in** according to some canonical order. **(zone enumeration problem)**
  - **RFC 5155**: "Instead of providing a range in which there are no hostnames, the DNS server uses a hashing function, and a signed range in which there are no valid hashes."

Practical DNSSEC Deployment

- In July 2010, DNSSEC root zone was signed
- In March 2011, .com was signed
- In January 2012, Comcast announced all DNSSEC service

- If you are a zone administrator (say for company.com), should you turn on DNSSEC? Benefit and cost?
  - Fraction of clients whose resolvers validate DNSSEC records
  - Fraction of clients which fail with DNSSEC
- Study by Lian et al. in 2013:
  - had 529,294 unique clients to connect them
  - “Less than 3% of clients failed to retrieve resources hosted on DNSSEC-signed domains with broken signatures.”

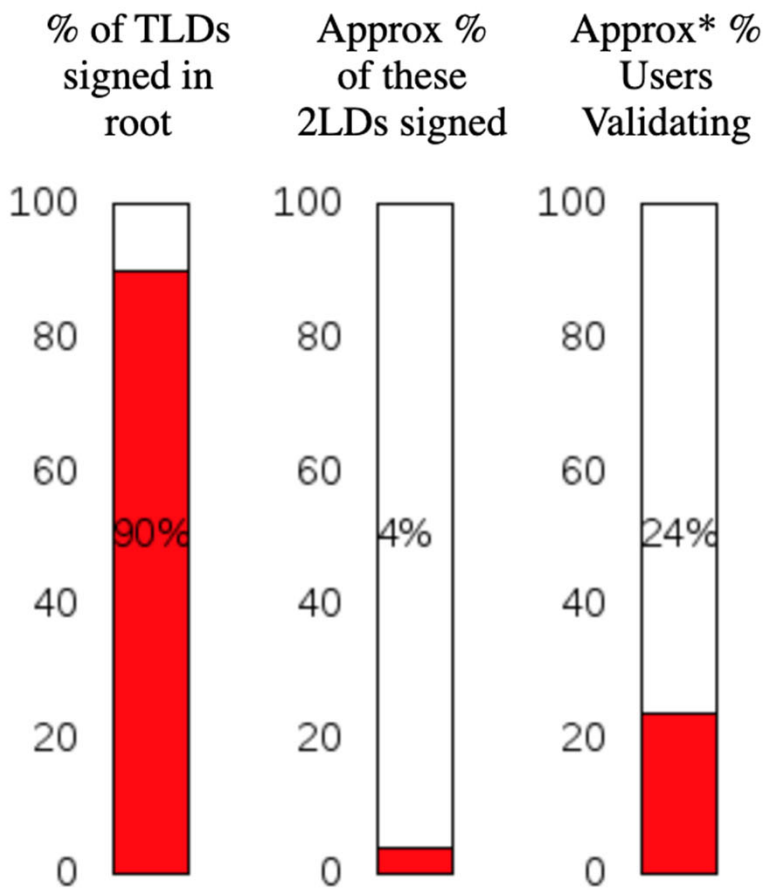
Lian, Wilson, et al. "Measuring the Practical Impact of DNSSEC Deployment." Presented as part of the 22nd USENIX Security Symposium (USENIX Security 13). 2013.

Why DNSSEC fails?

- Large DNS response size
  - TCP fallback triggered
  - Some networks filter TCP-based DNS responses
- Some users/browsers ignore DNSSEC invalid messages
  - Usability vs. security

DNSSEC Deployment Report

Wed Mar 4 03:06:49 PST 2020
Total TLDs: 1516 / Signed TLDs in root: 1376 / Recently added: xn--q7ce6a. (01/30/2020)



(source: http://rick.eng.br/dnssecstat/)

CONFIDENTIALITY OF DNS

Mass Surveillance Attacks (or Pervasive Monitoring)

- State-sponsored adversaries monitor a large portion of the Internet
  - NSA's QuantumDNS (2014) and MoreCowBell (2015) projects
  - pervasive (non-selective) collection of metadata; e.g., 40% of traffic of UK is monitored
- DNS packets can be very attractive metadata
  - universally used, unencrypted, privacy sensitive

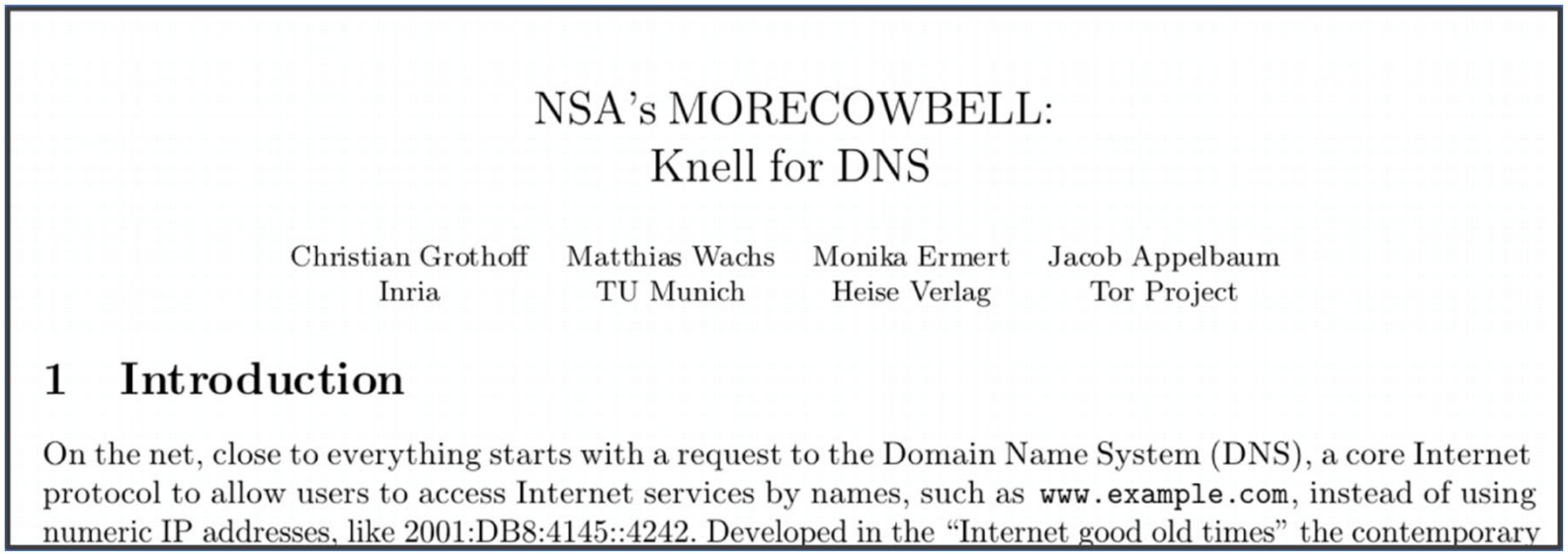
Utah data center

DNS Privacy

- People could be watching our queries.

RFC 7626 on DNS privacy

> The revelations (from the Edward Snowden documents, which were leaked from the National Security Agency (NSA)) of the MORECOWBELL surveillance program [morecowbell], which uses the DNS, both passively and actively, to surreptitiously gather information about the users, is another good example showing that the lack of privacy protections in the DNS is actively exploited.



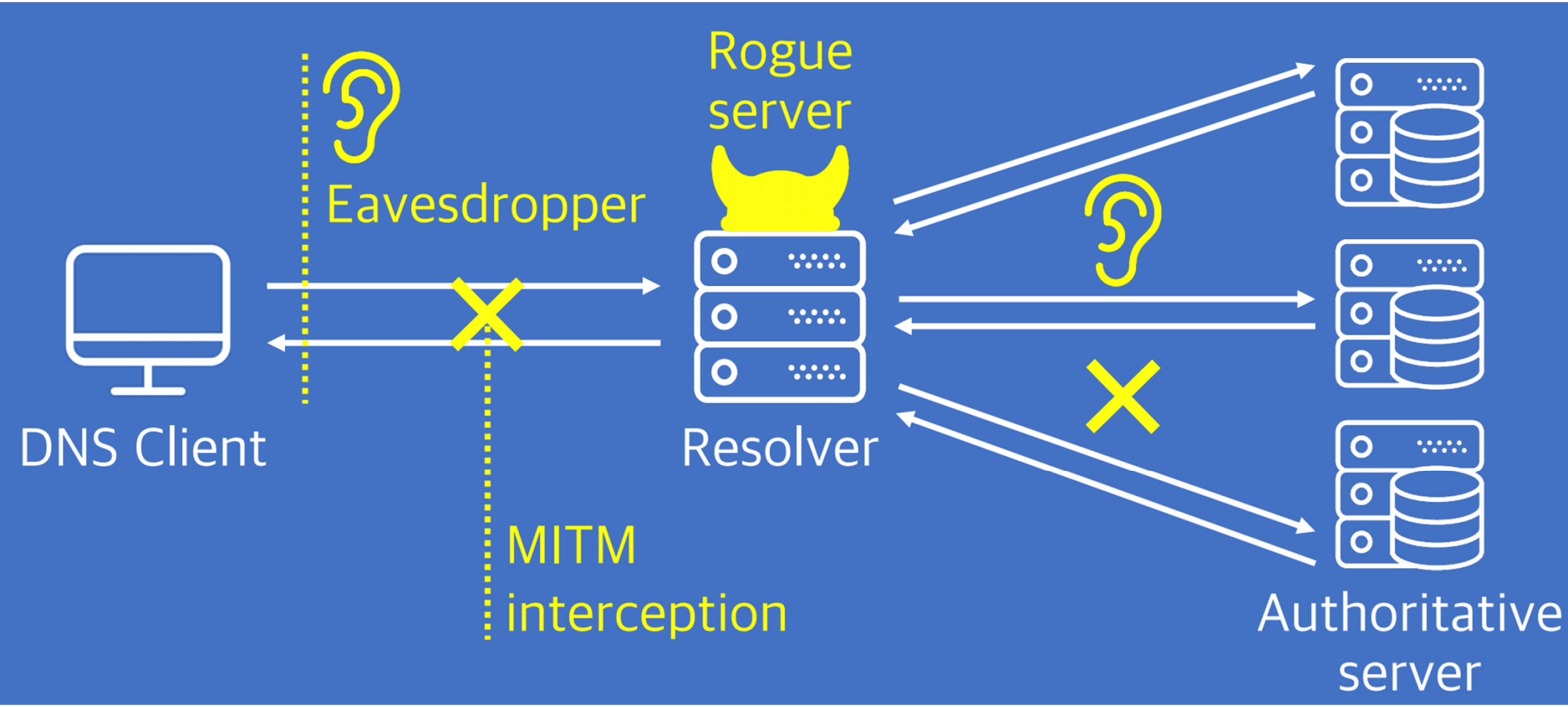
NSA's MORECOWBELL:
Knell for DNS

Christian Grothoff, Inria
Matthias Wachs, TU Munich
Monika Ermert, Heise Verlag
Jacob Appelbaum, Tor Project

1 Introduction

On the net, close to everything starts with a request to the Domain Name System (DNS), a core Internet protocol to allow users to access Internet services by names, such as `www.example.com`, instead of using numeric IP addresses, like 2001:DB8:4145::4242. Developed in the "Internet good old times" the contemporary

DNS Privacy



(source: Chaoyi Lu's Sigcomm presentation slides)

By watching DNS queries, an adversary could do user tracking [Kirchler 2016], user behaviour analysis [Kim 2015], etc.

DNS over Encryption Protocols (1)

- DNS-over-TLS (DoT)
  - Standardized in RFC 7858
  - Clients and servers negotiate a TLS session before DNS lookup
  - Uses port 853 (Easy to distinguish from other TLS traffic)
  - Supported by OS, DNS software, and large DNS resolvers (e.g., Google)

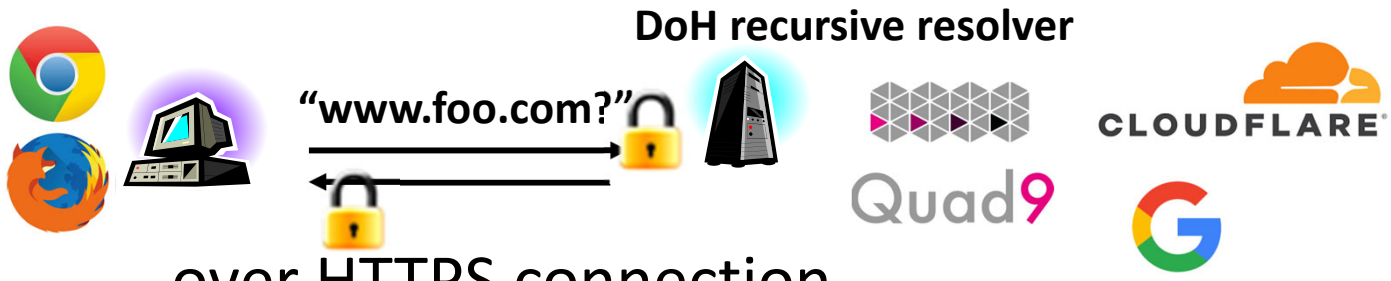
- DNS-over-DTLS
  - Works on UDP for better performance
  - Designed only for backup proposal for DoT and no real-world implementation

DNS over Encryption Protocols (2)

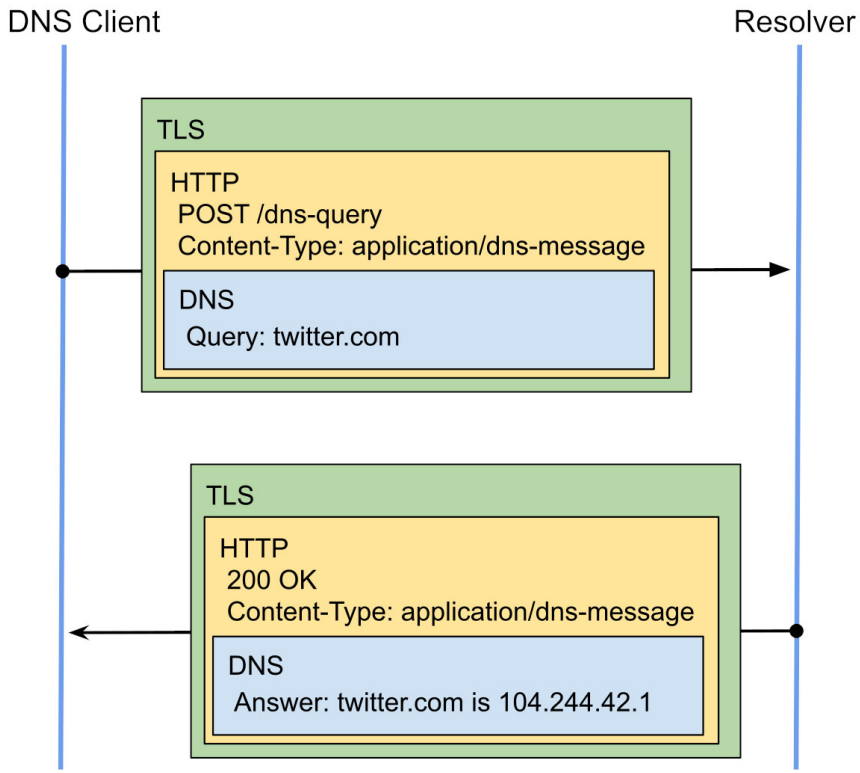
- DNS-over-HTTPS (DoH)
  - Standardized in RFC 8484
  - 2 application layer protocols (HTTP and DNS) are leveraged.
  - Embed DNS queries into HTTPS message
    - Utilizes URI template
    - DNS query is encoded in URI parameter (GET) or HTTP message body (POST)
  - Can mix DNS query with other HTTPS traffic
  - Need different implementation of DNS software
  - Supported by large resolvers including Google, Cloudflare

Setting in Firefox browser

DNS-over-HTTPS overview



over HTTPS connection

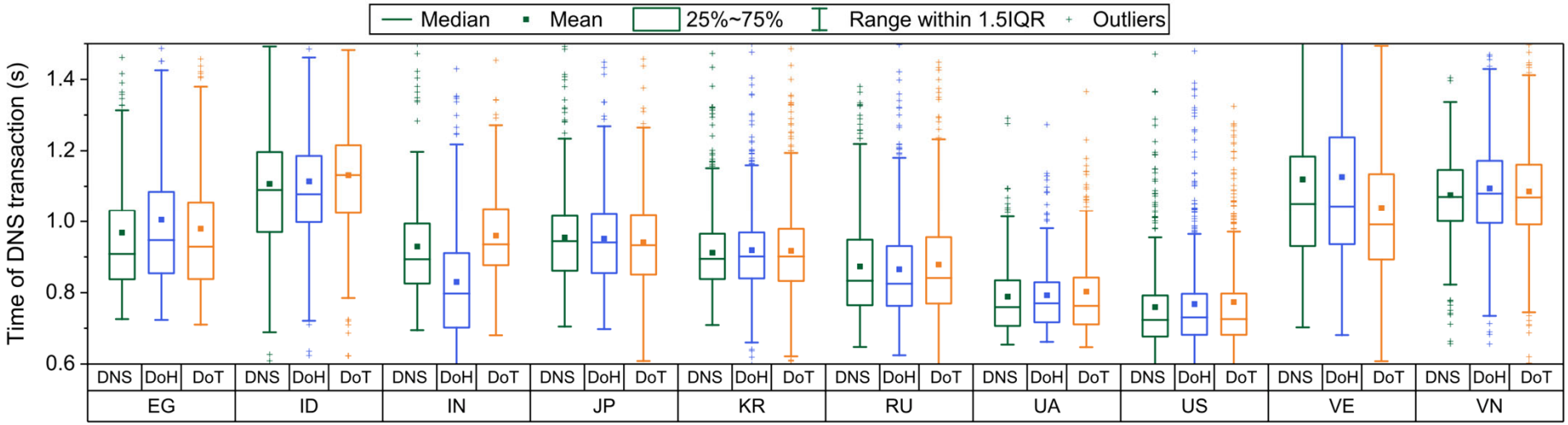


DNS-over-Encryption: Challenges

- Performance
  - Increased latency
- Deployment / enrollment
  - Difficult to bootstrap
- Security
  - Lack of clear trust model
- Privacy and policy
  - Enforcing local policy on DoH users
  - Reliance on a few global providers

Performance

- Latency:
  - Problem: DoH requires a HTTPS handshake to begin with (~ 2-3 RTT)
  - Solution: reuse established HTTPS sessions for DNS
    - When connection is reused, performance overhead on query time is tolerable.



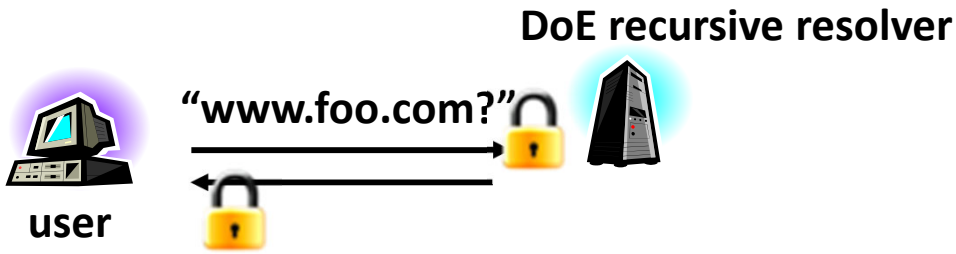
DNS-over-HTTPS is becoming a de facto standard (as of March 2020)

- Bootstrap: "How to transition from DNS to DoH?"
  - Starting with major browsers (e.g., Firefox, Chrome)
  - And major cloud vendors (e.g., Google, Cloudflare, Quad9)

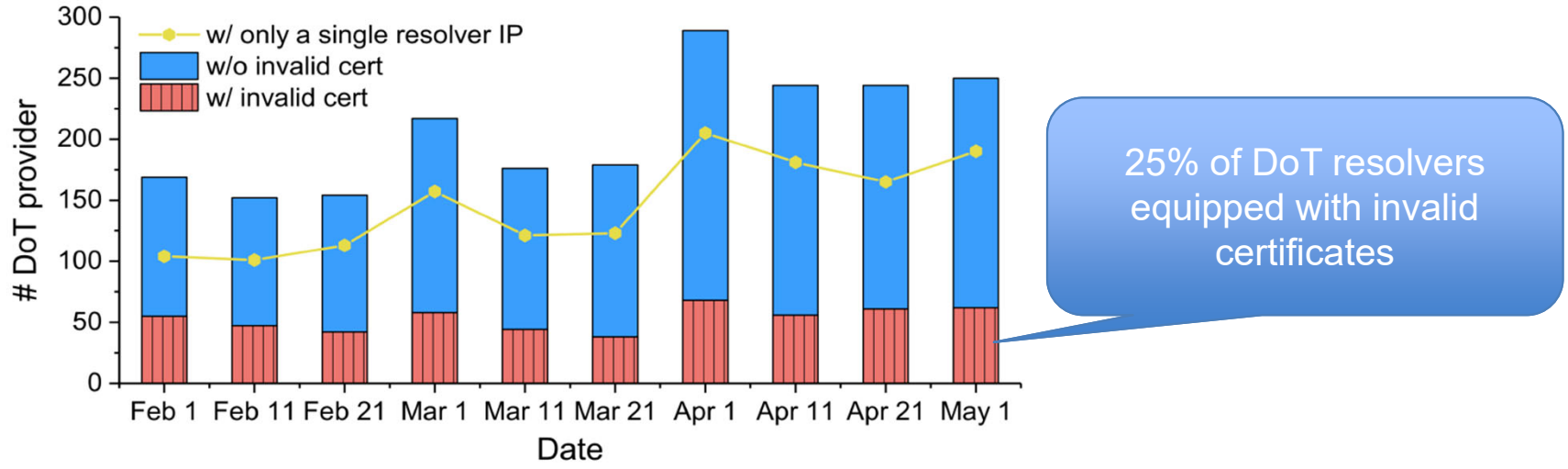
Table 1: Comparison of different DNS-over-Encryption protocols

Category	Criterion	DNS-over-TLS	DNS-over-HTTPS	DNS-over-DTLS	DNS-over-QUIC	DNSCrypt
Protocol Design	Uses other application-layer protocols	○	●	○	○	●
	Provides fallback mechanism	●	○	●	●	○
Security	Uses standard TLS	●	●	●	●	○
	Resists DNS traffic analysis	◐	●	◐	◐	●
Usability	Minor changes for client users	◐	●	○	○	◐
	Minor latency above DNS-over-UDP	◐	◐	●	●	◐
Deployability	Runs over standard protocols	●	●	●	○	○
	Supported by mainstream DNS software	●	◐	○	○	◐
Maturity	Standardized by IETF	●	●	●	○	○
	Extensively supported by resolvers	●	●	○	○	◐

Lack of clear trust model



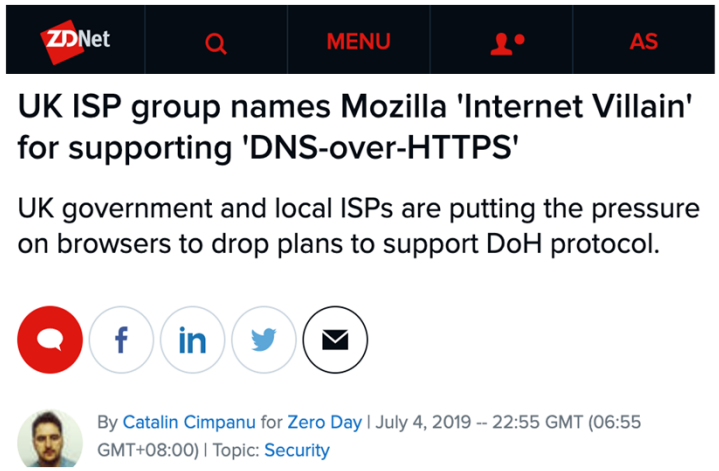
- How to find a DoE resolver in the first place?
- Trust model: "Are you who you claim to be?"
  - SSL PKI should be correctly configured at the resolvers and checked by users



Reachability of DoH servers

Vantage	Resolver	Query Failure Rate	
		DNS/TCP	DoH
Global	Cloudflare	16.5%	0.1%
	Google	15.9%	0.2%
	Quad9	0.2%	14.0%
China	Google	1.1%	99.9%

- DoH is widely allowed by local ISPs (except Google in China)
  - ✓ Is this a sign of smooth transition from DNS to DoH?



Why?

Big shift of power over DNS: from local networks to global vendors

- Historically, most of DNS resolvers have been operated by local ISP/campus/enterprise networks
  - Dynamic Host Configuration Protocol (DHCP) usually configures a local DNS resolver
- Few tach-savvy users may customize (e.g., 8.8.8.8 or OpenDNS)
  - Yet, local network can still manipulate plaintext DNS
- Therefore, ***local authorities*** or ***enterprises*** could:
  - ***DNS-based filtering***: some states mandate DNS filtering to block access to harmful contents, such as child pornography, extremist movement

✓ ***Privacy of domain names vs. Protection for local communities***

Highly anticipated battle over DNS

- Browsers do want to expand DoH to all Internet users
- ISPs may actively disrupt DoH traffic
  - But, DoH packets look like regular HTTPS packets
  - How to disrupt?
- Government's monitoring on terrorist activities may be affected.
- Malware starting to use DoH for their command-and-control channels. Surely, we will see more in the future.
  - E.g., https://santanderglobaltech.com/en/how-to-protect-from-malware-that-abuses-dns-over-https-doh/
- Only a small number of global vendors collect all our DNS data. Is this acceptable?

We will see more discussion on this issue in the near future…

Summary

- DNS is one of the most fundamental Internet services
- Yet, problems in all CIA properties
- Name record integrity is crucial
  - Can be exploited by scammers
  - DNSSEC to the rescue
    - Yet, the adoption has been slow
    - Complicated issues; e.g., security, usability, deployability…
- Confidentiality due to privacy concerns
  - DNS over HTTPS is becoming a de facto standard
  - Yet, many security/privacy concerns exist

Questions?

Next week:
Routing Security

Two papers

- **A Study of Prefix Hijacking and Interception in the Internet (Sigcomm'07)**

- **SCION: Scalability, Control, and Isolation On Next-Generation Networks (IEEE S&P'11)**