A Comprehensive Study of DNS-over-HTTPS Downgrade Attack

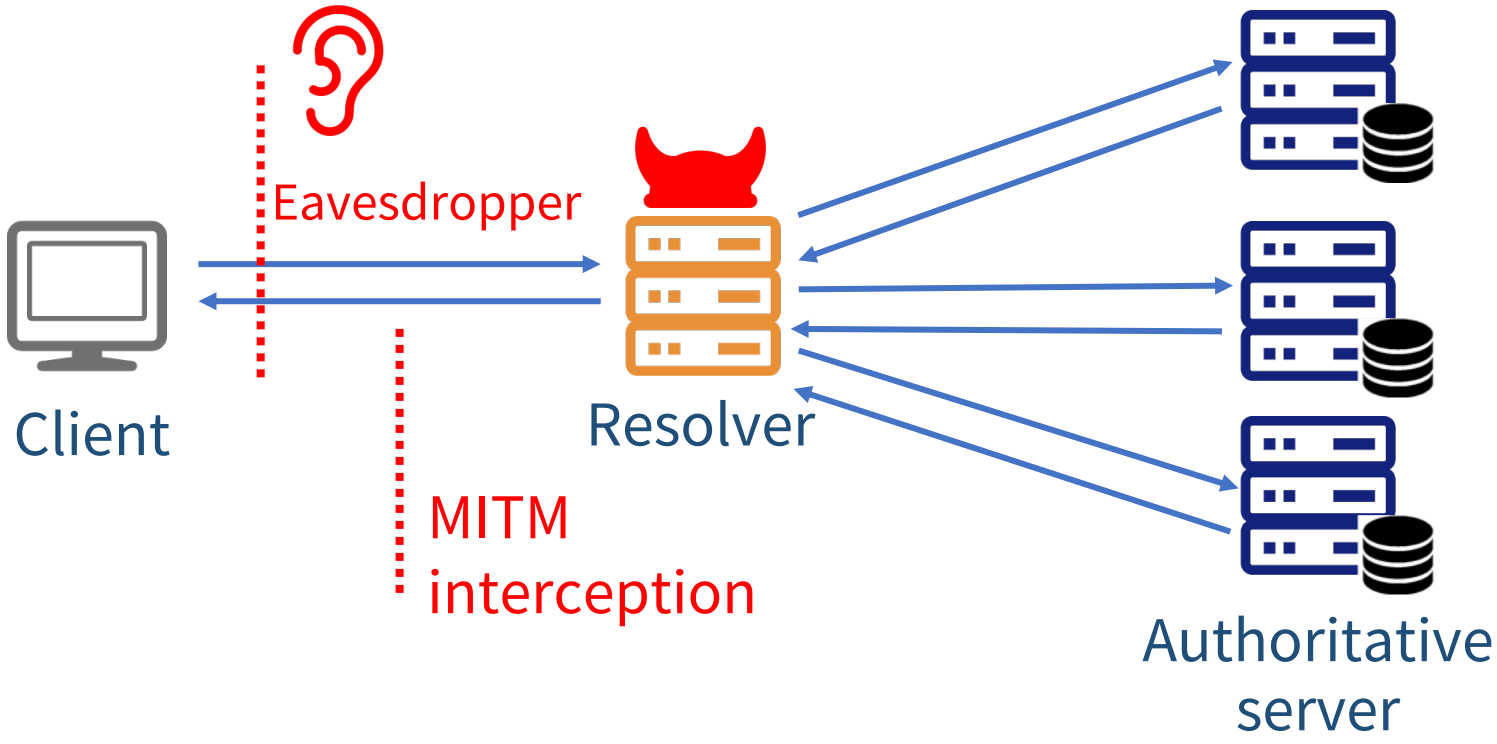
Qing Huang, Deliang Chang, Zhou Li

UCI University of California, Irvine

清華大學 Tsinghua University

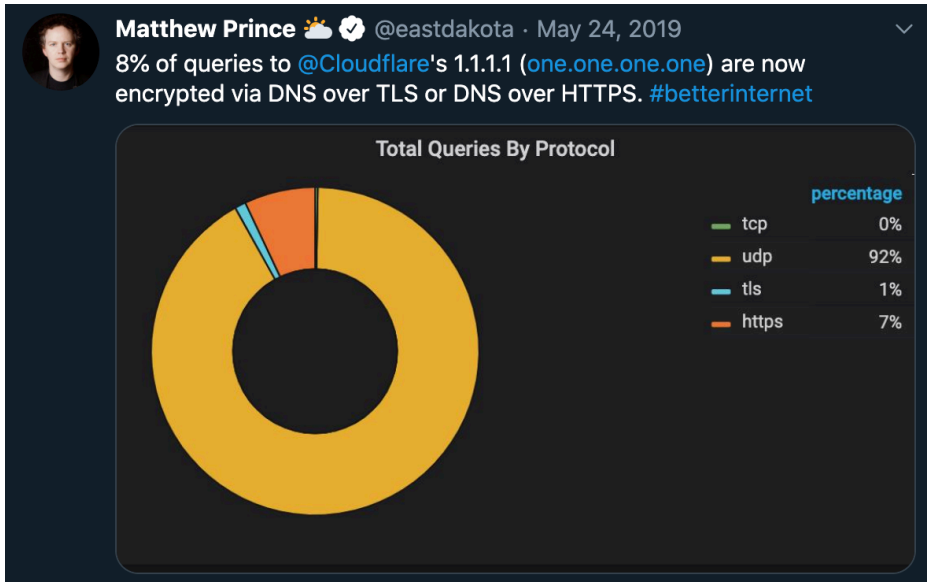
DNS Privacy

Where are the risks?



DoH Service Support

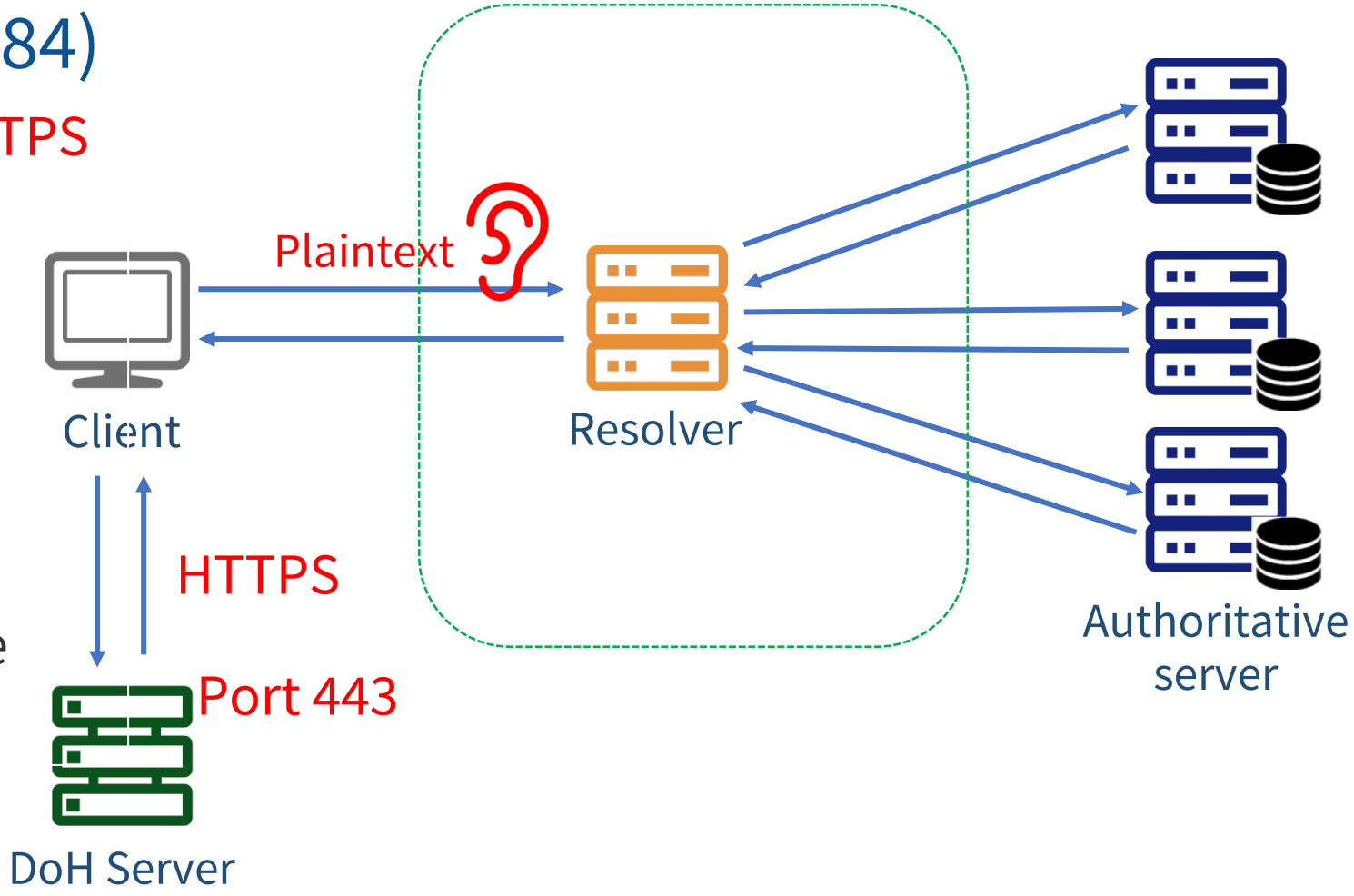
- Most promising
  - Up to 7% of its queries have been encrypted using DoH
- Widely Support
  - Several large public DNS resolvers, operating systems and browser vendors have implemented DoH



DoH server	URI
Google	https://dns.google/dns-query
Cloudflare	https://cloudflare-dns.com/dns-query https://chrome.cloudflare-dns.com/dns-query
Quad9	https://dns.quad9.net/dns-query
Umbrella/OpenDNS	https://doh.opendns.com/dns-query
CleanBrowsing	https://doh.cleanbrowsing.org/doh/family-filter/
Comcast	https://doh.xfinity.com/dns-query
DNS.SB	https://doh.dns.sb/dns-query

DNS over HTTPS (DoH, RFC 8484)

- Overview of DoH (RFC 8484)
  - Embeds DNS packets into HTTPS messages.
  - Shared port 443
- Usage profile
  - **Strict** privacy profile
  - **Opportunistic** privacy profile



Will the DoH ensure that user privacy is protected?

Will the DoH ensure that user privacy is protected?

NO!

Downgrade in DNS-over-HTTPS

- Definition
  - Force a system to abandon its high-standard security protocol and fallback to an older, weaker one.
  - DoH → DNS (udp)

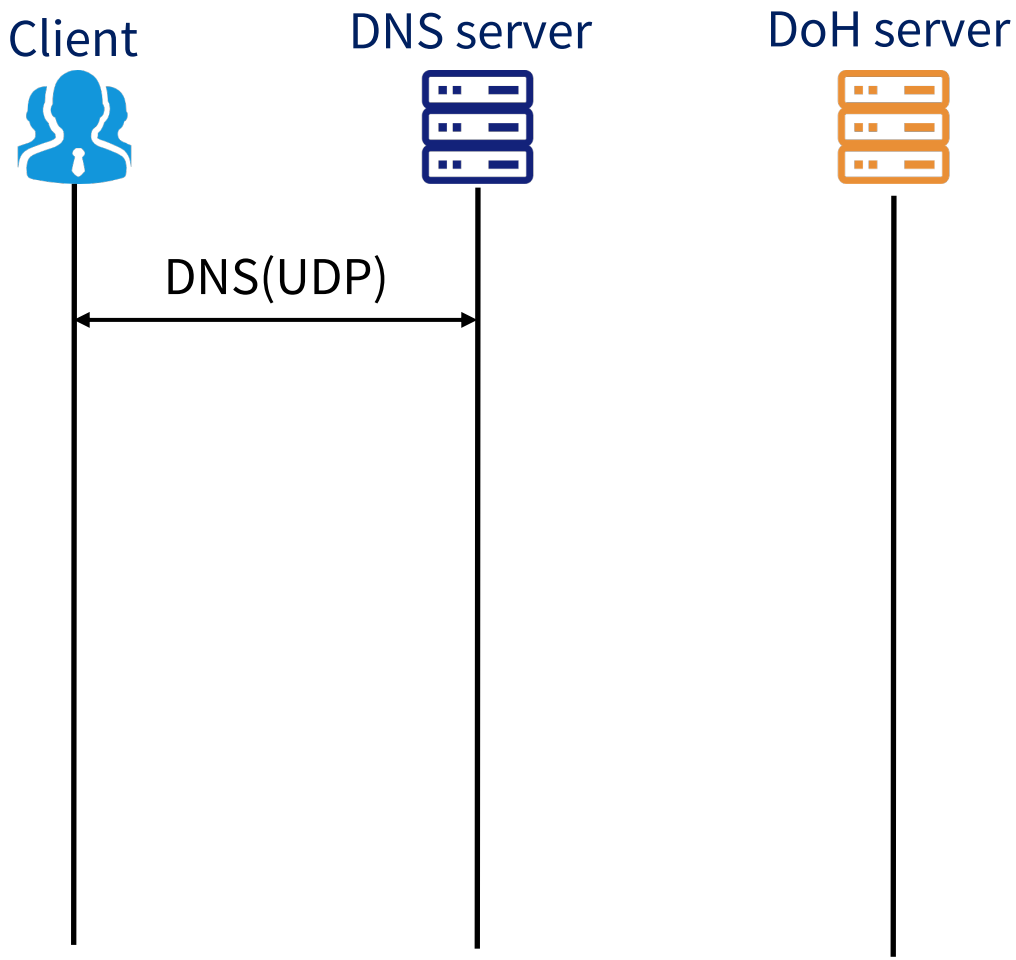
- Vulnerable to be attacked
  - Adversary might try to downgrade DoH to DNS and carry out the known DNS attacks

Research Gaps

- Research questions
  - Attack vectors of DoH downgrade
  - Browser reaction under attack (Defend?)
  - Harmfulness?
  - Improvement

DoH Resolution Process

- Phase1: URI Resolution
  - Browser sends an unencrypted DNS request to resolve the URI and obtain the IP address of the DoH server



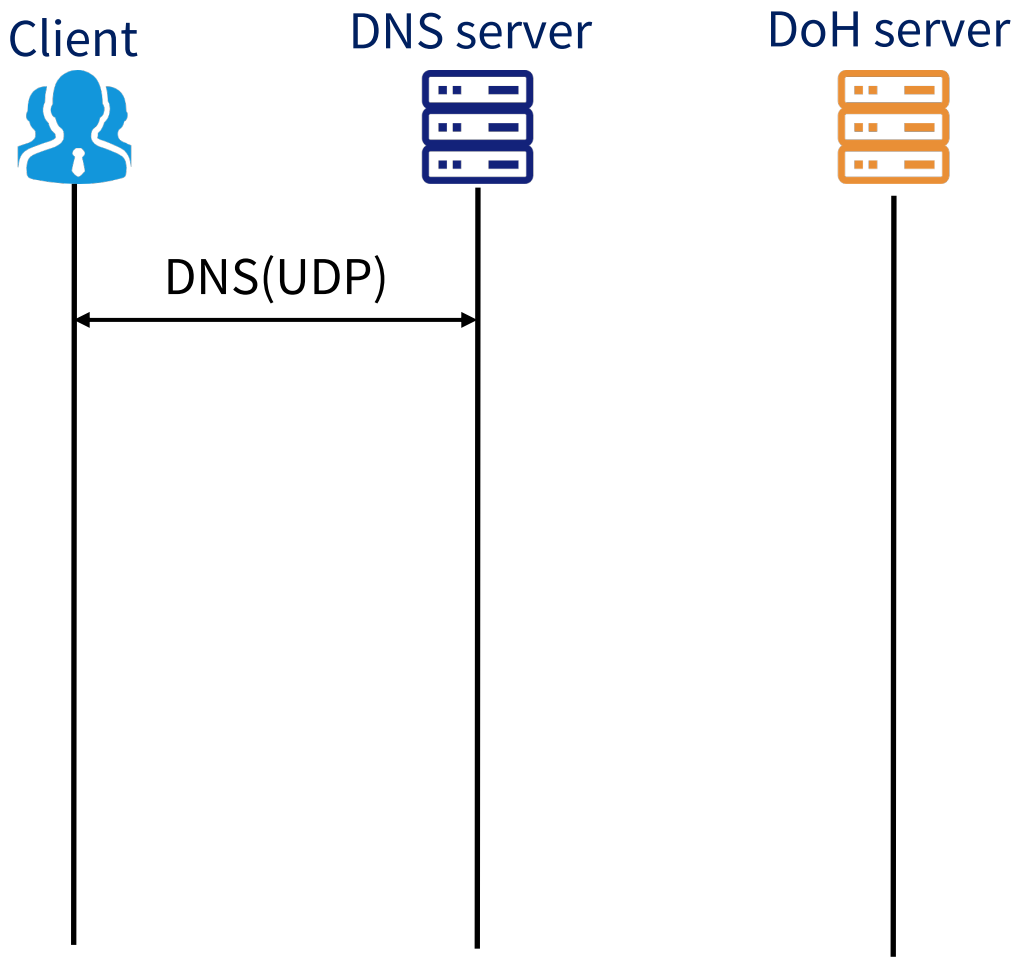
DoH Resolution Process

- Phase1: URI Resolution

  Example: https://dns.quad9.net/dns-query → dns.quad6.net

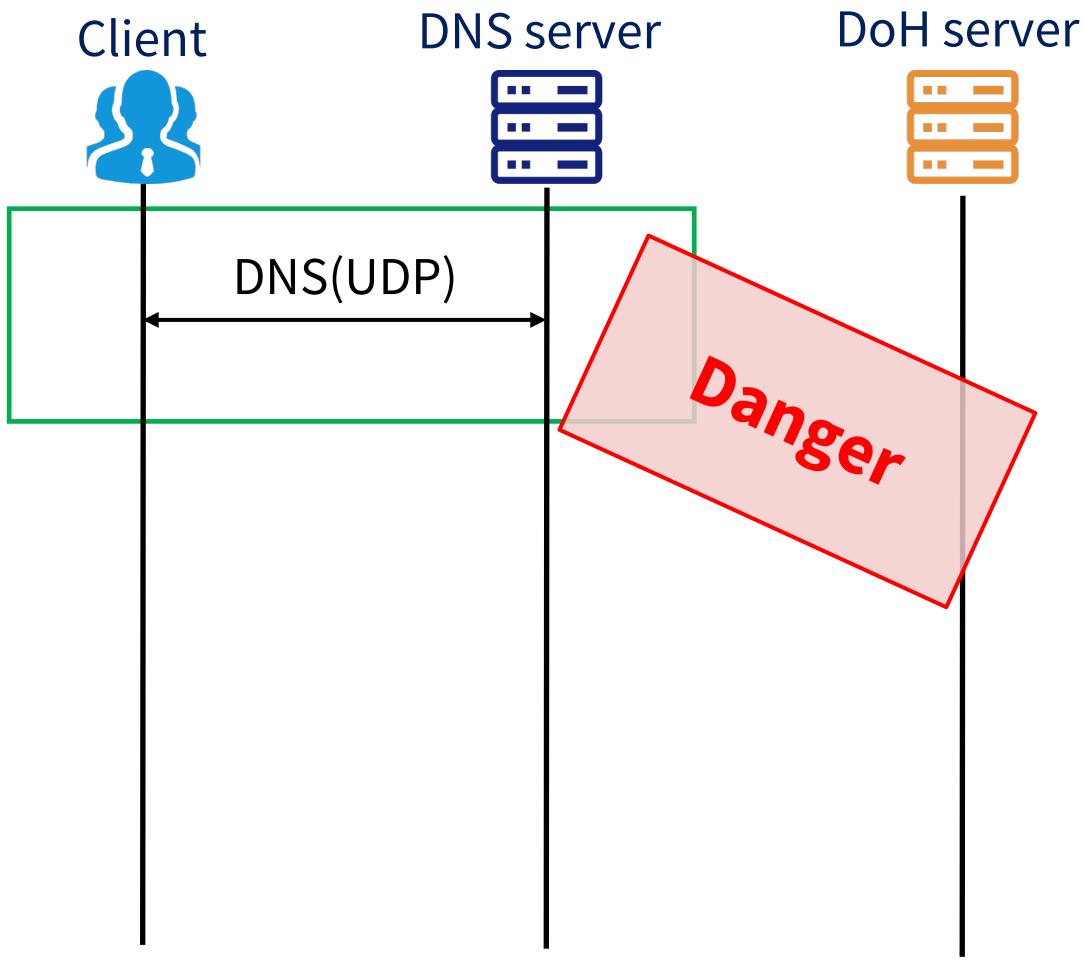
  dns.quad6.net

  → 9.9.9.9 or 149.112.112.112



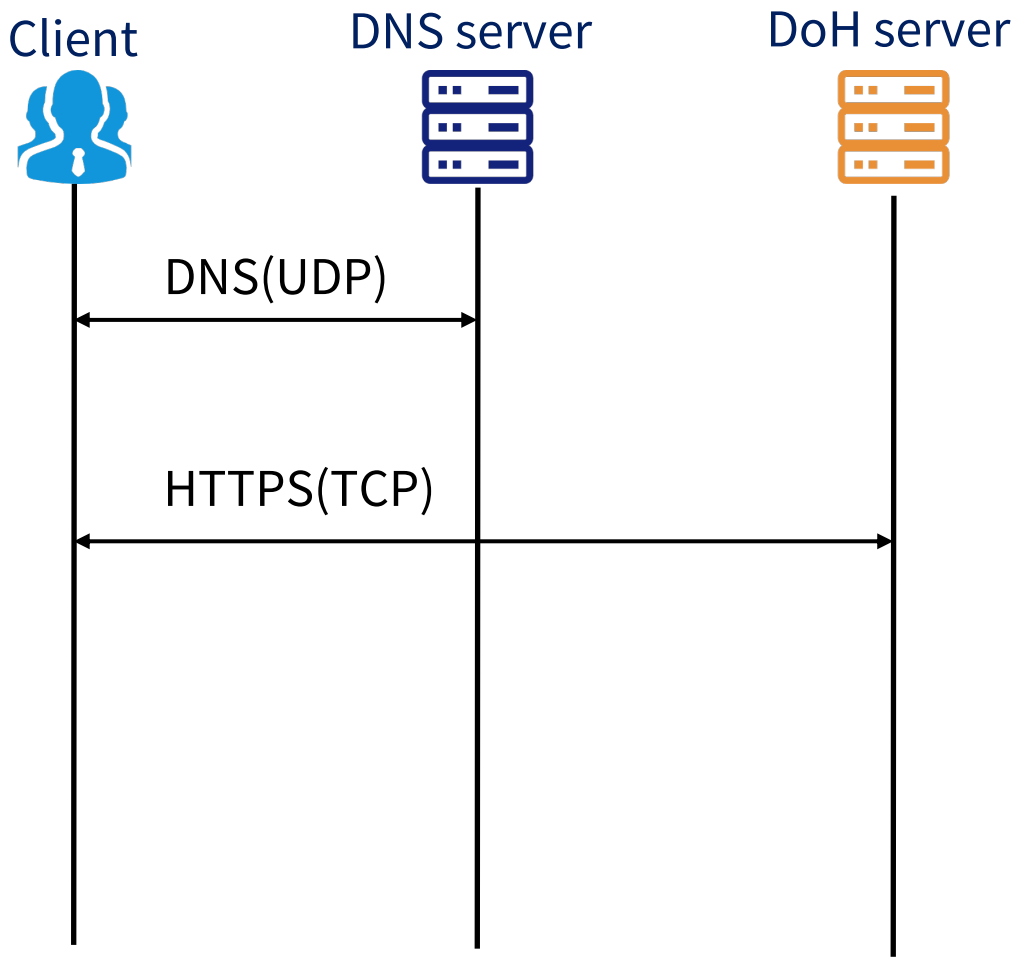
DoH Resolution Process

- Phase1: URI Resolution
  - Same as the traditional DNS resolution process
  - Any attacker can view the plain text content in the DNS packet and tamper it



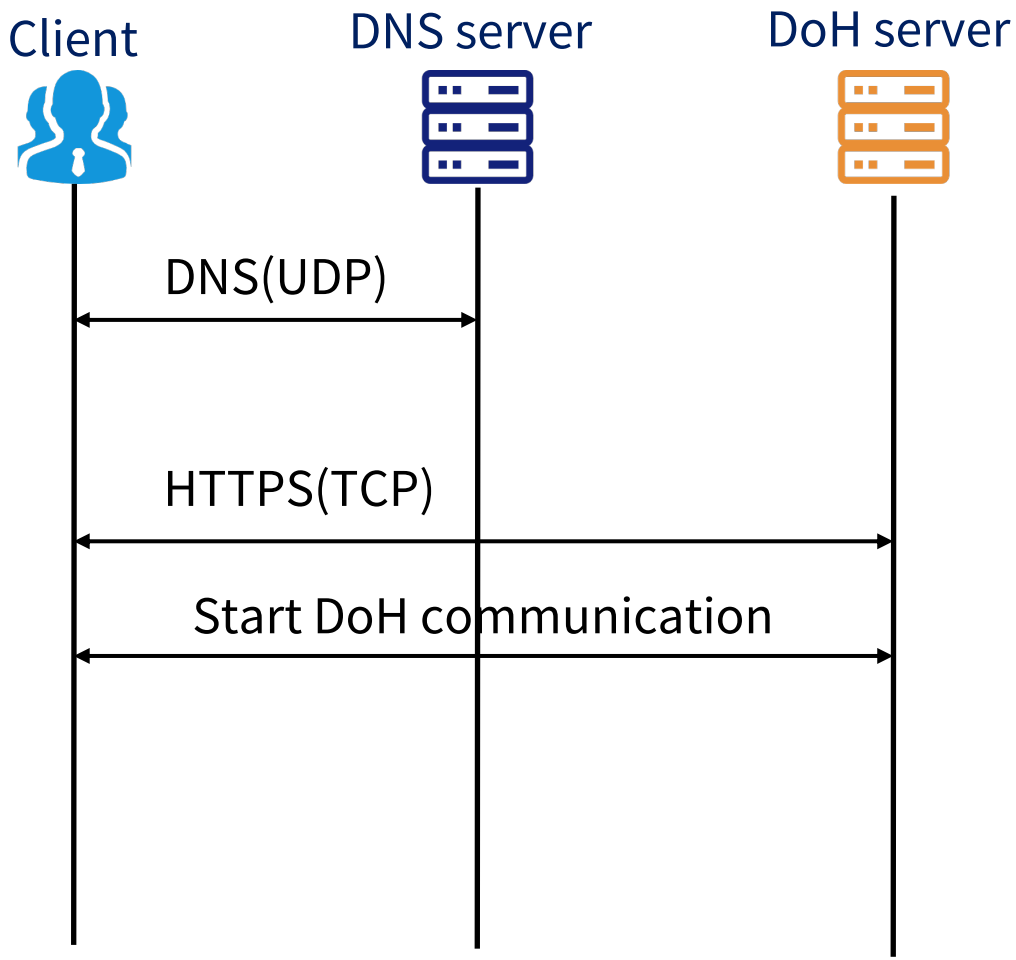
DoH Resolution Process

- Phase2: Connection & Communication
  - Browser establishes a secure connection with the DoH resolver via TLS



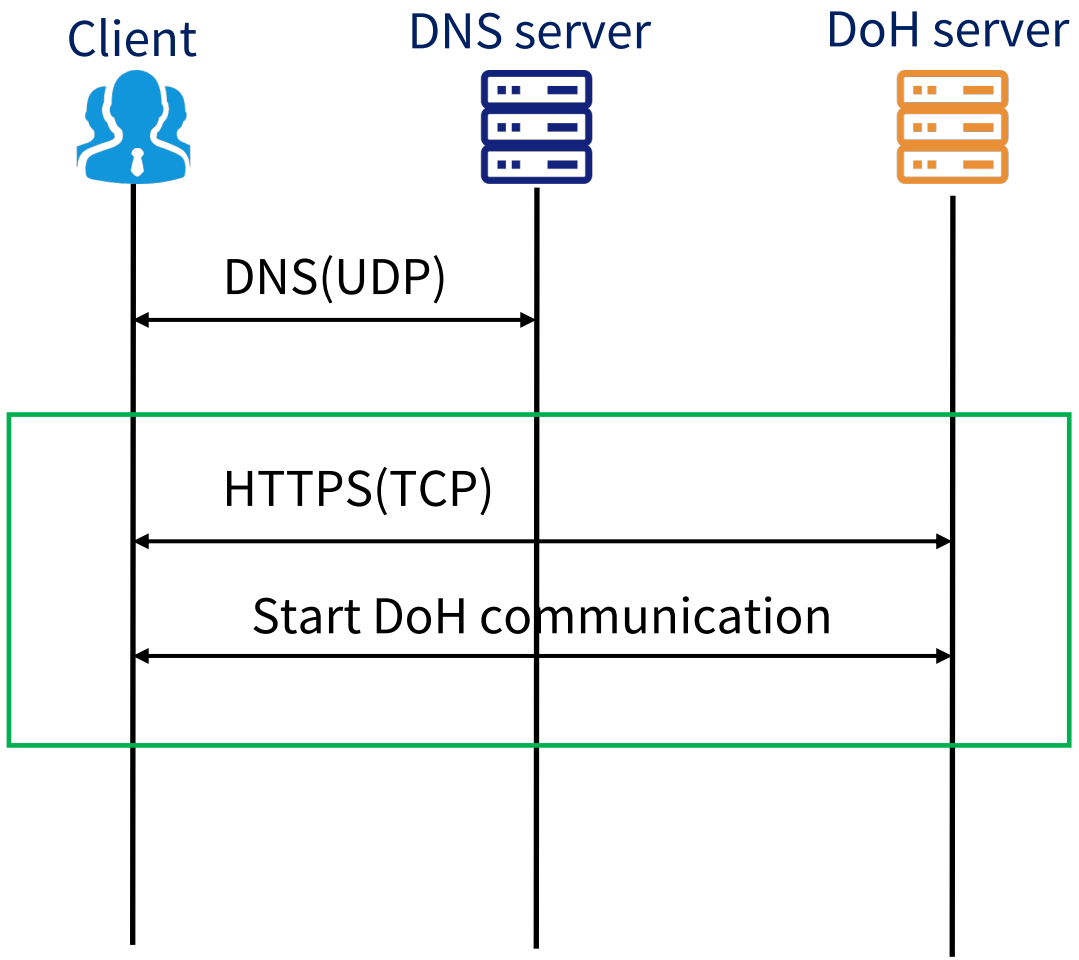
DoH Resolution Process

- Phase2: Connection & Communication
  - DNS request will be encapsulated in an encrypted HTTPS packet through this transmission channel



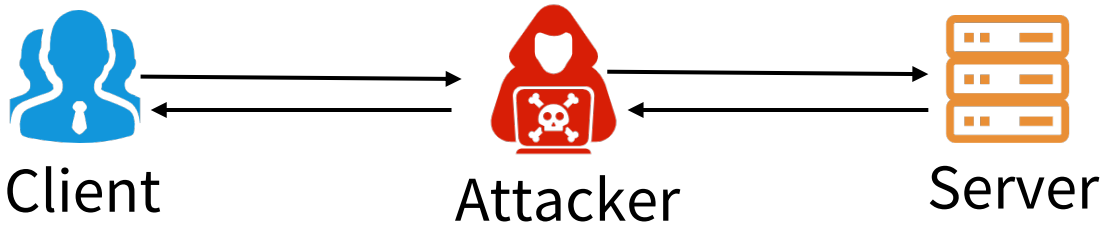
DoH Resolution Process

- Phase2: Connection & Communication
  - Browser establishes a secure connection with the DoH resolver via TLS
  - DNS request will be encapsulated in an encrypted HTTPS packet through this transmission channel

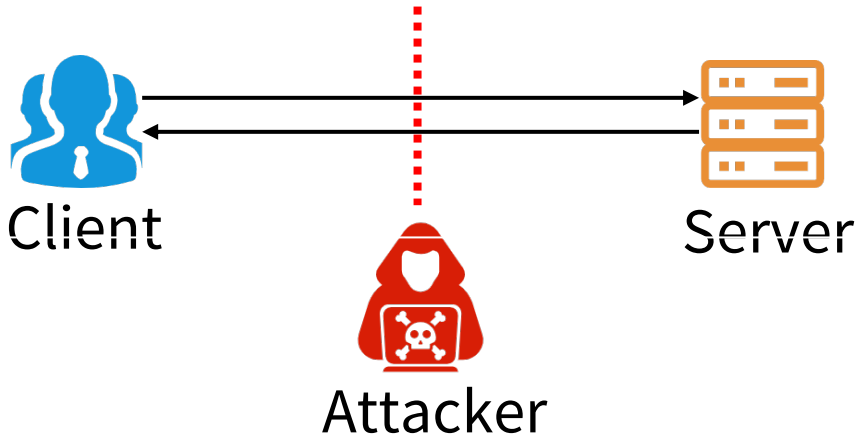


Adversary Model

- In-path Attacker
  - Inspect the traffic of the victim
  - Have the ability to modify all packets from and towards the victim.



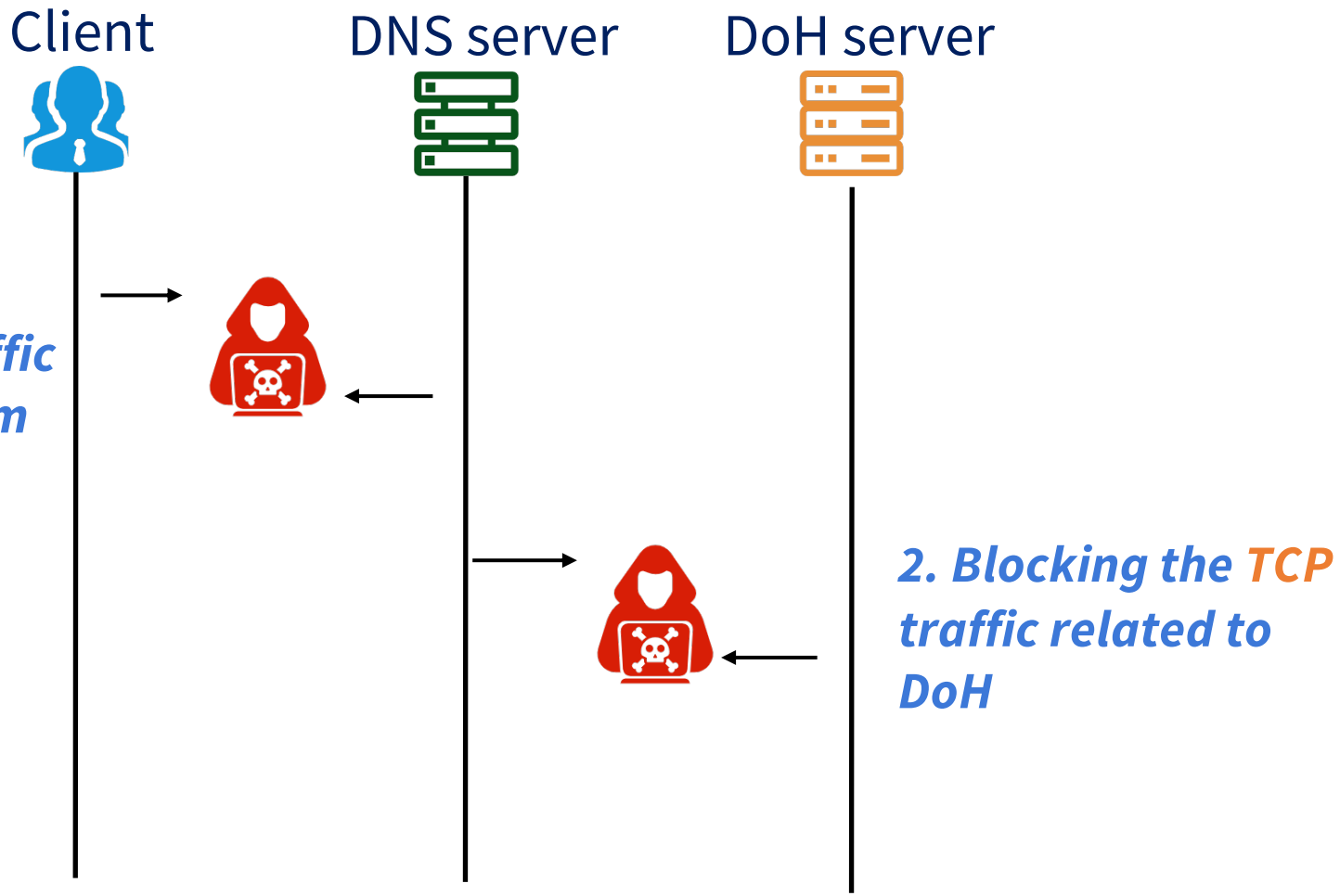
- On-path Attacker
  - Inspect the traffic of the victim
  - Inject new packets



Downgrade Attack Method

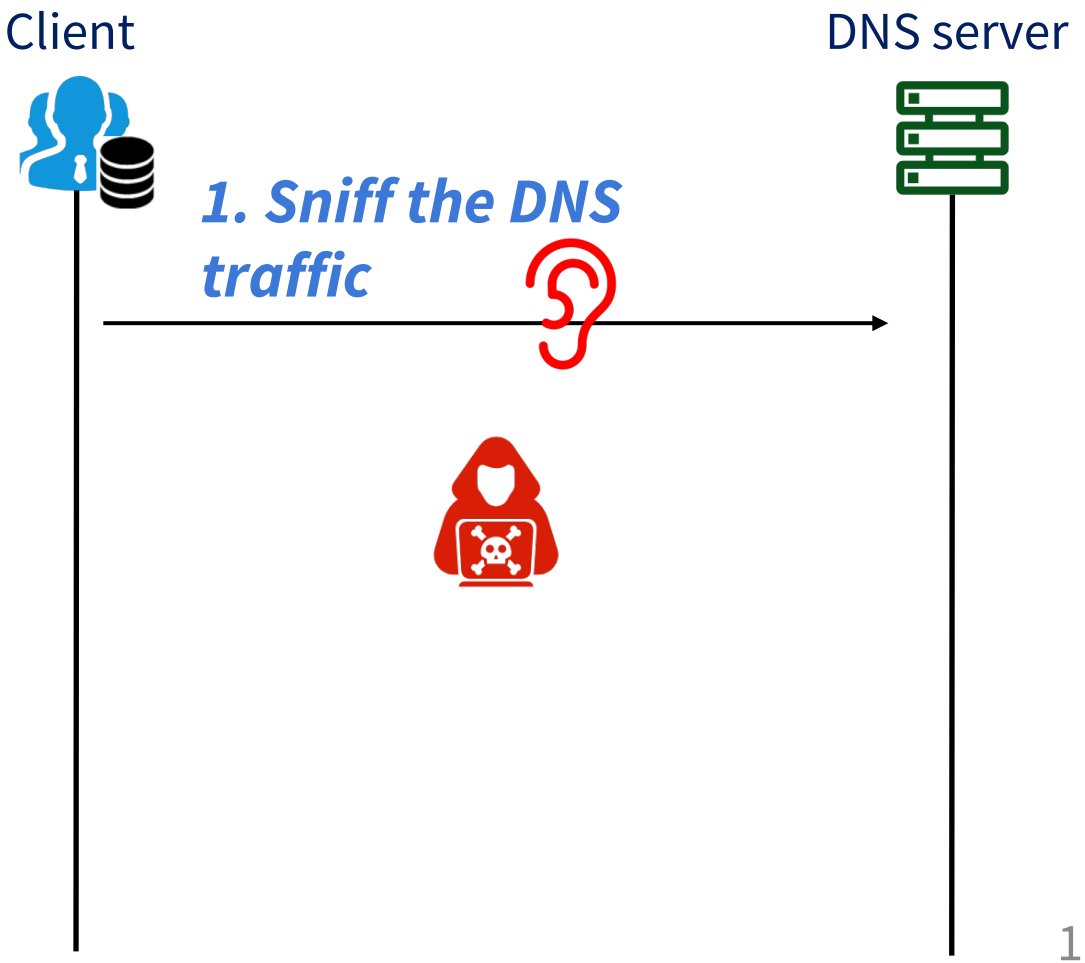
- DNS Traffic Interception & TCP Traffic Interception

In-path Attacker



Downgrade Attack Method

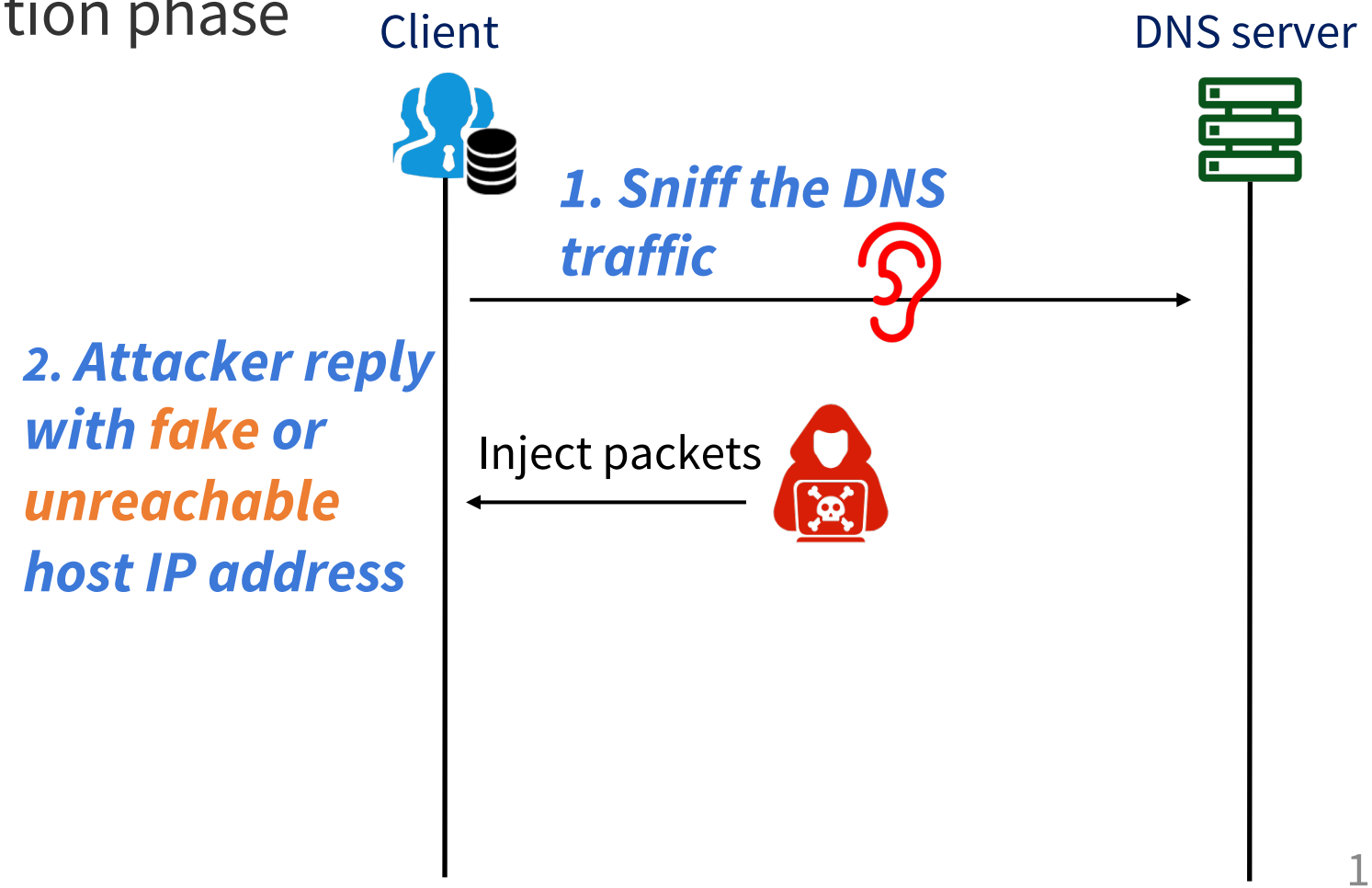
- DNS Cache Poisoning
  - Target URI resolution phase



On-path Attacker

Downgrade Attack Method

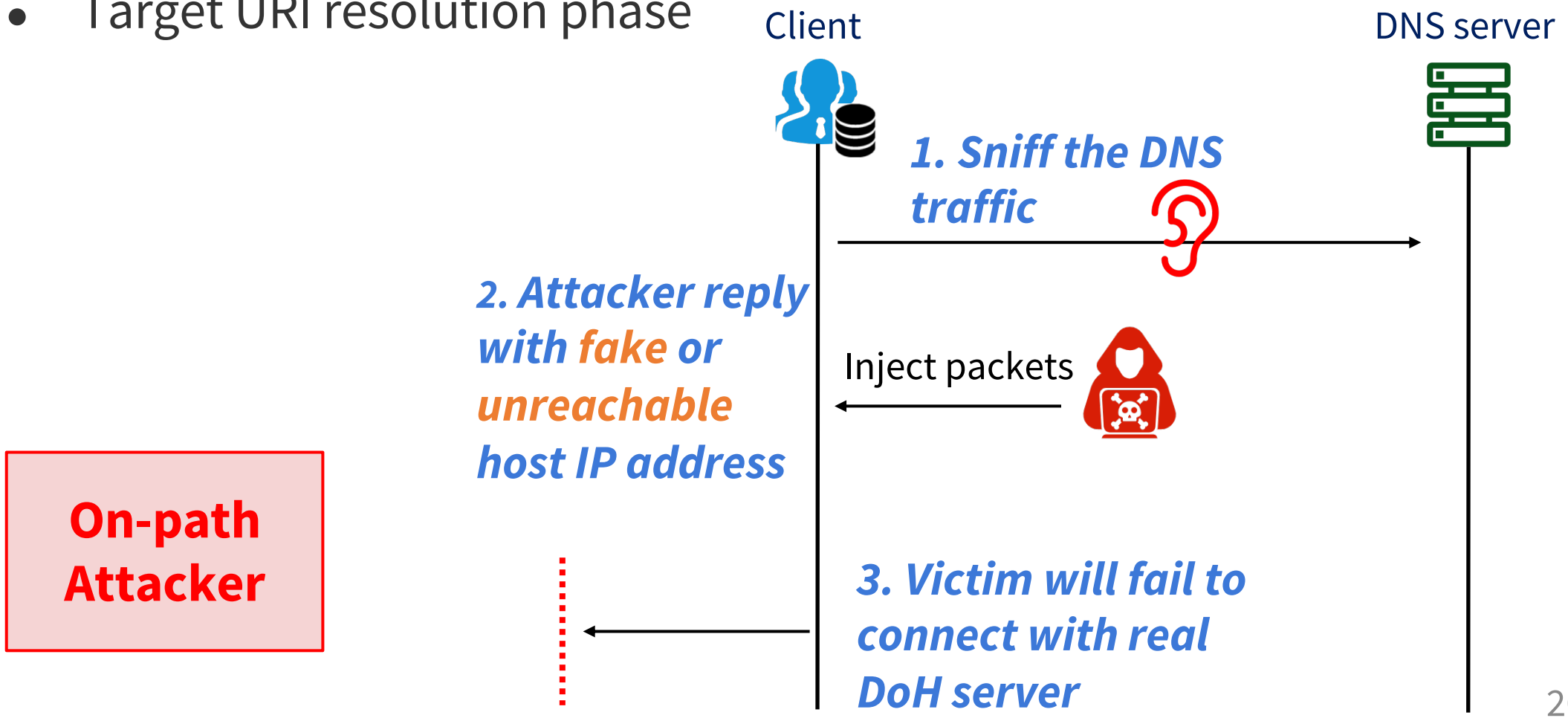
- DNS Cache Poisoning
  - Target URI resolution phase



On-path Attacker

Downgrade Attack Method

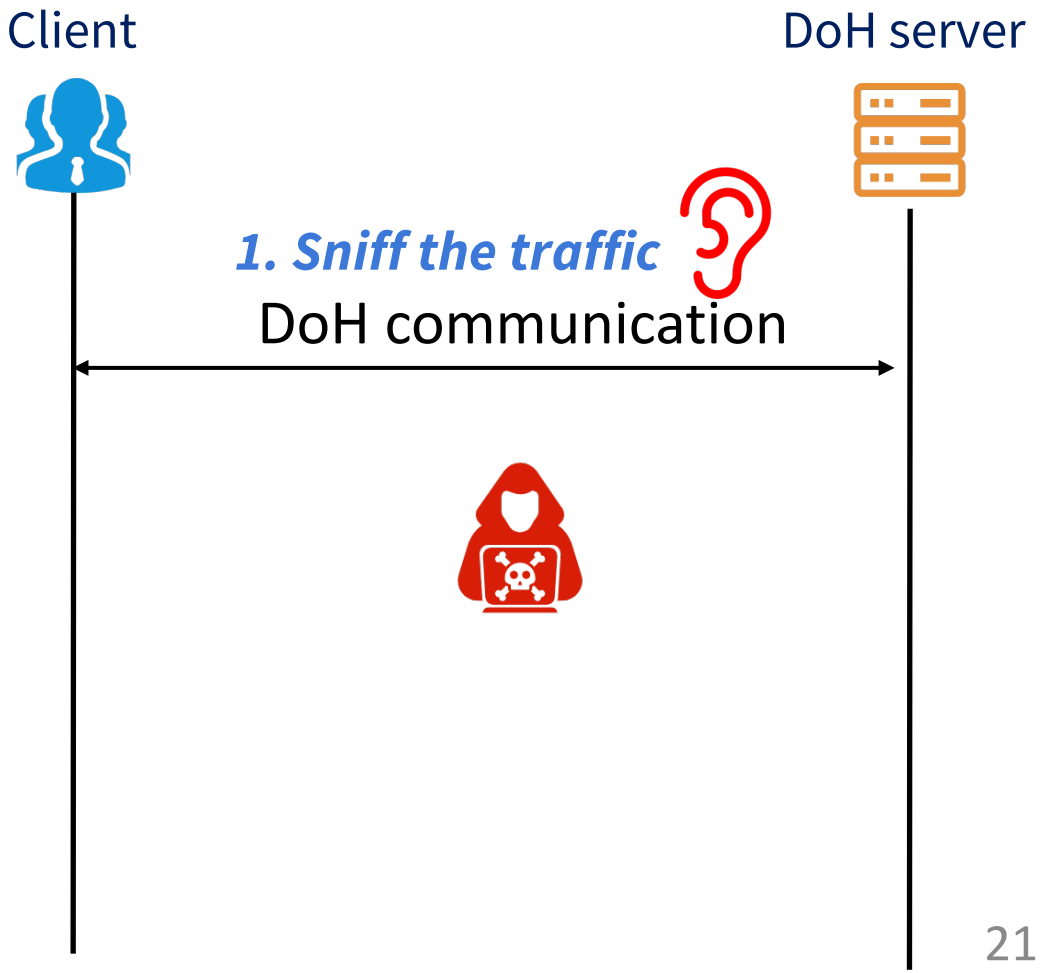
- DNS Cache Poisoning
  - Target URI resolution phase



Downgrade Attack Method

- TCP Reset Attack
  - Target URI resolution phase

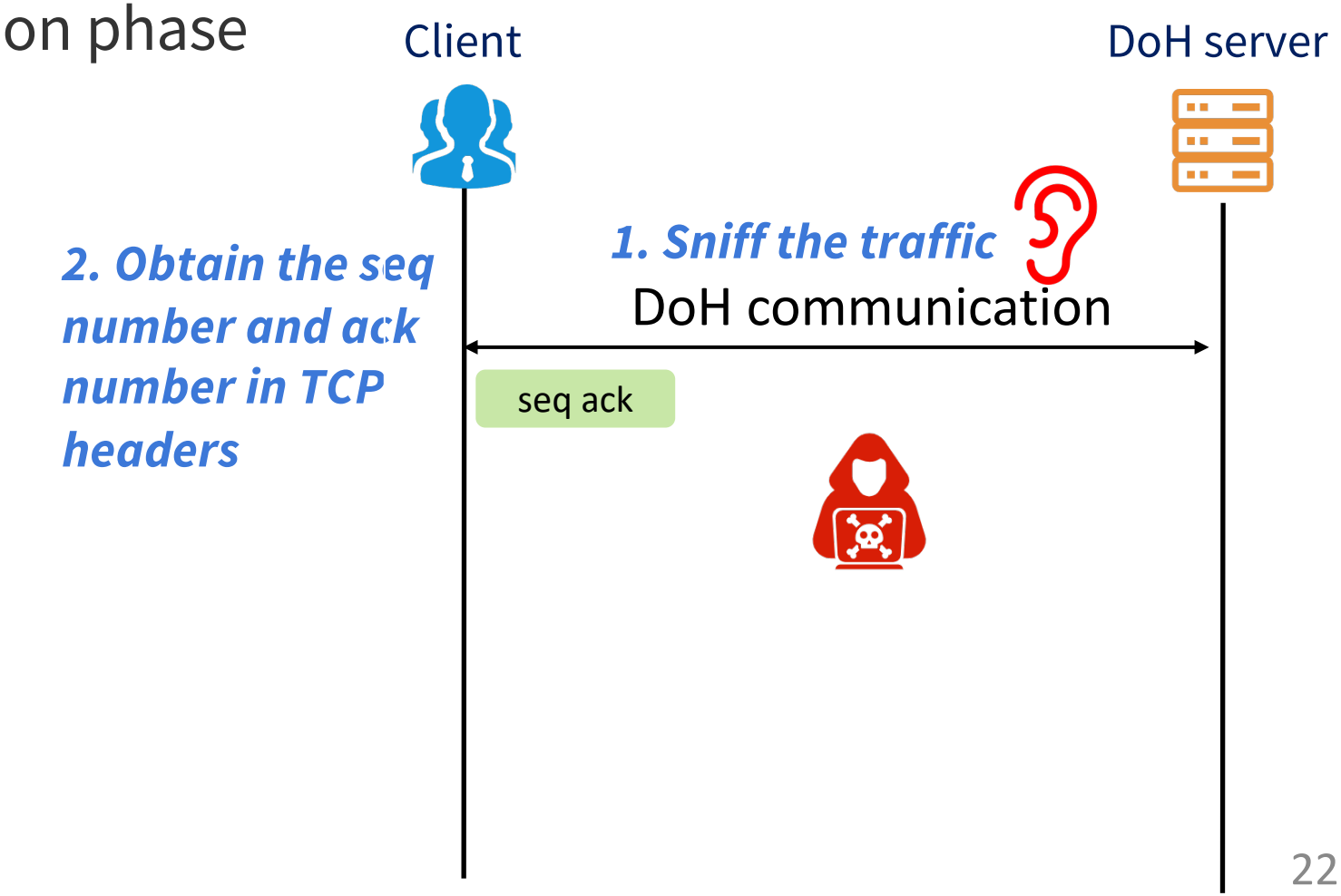
On-path Attacker



Downgrade Attack Method

- TCP Reset Attack
  - Target URI resolution phase

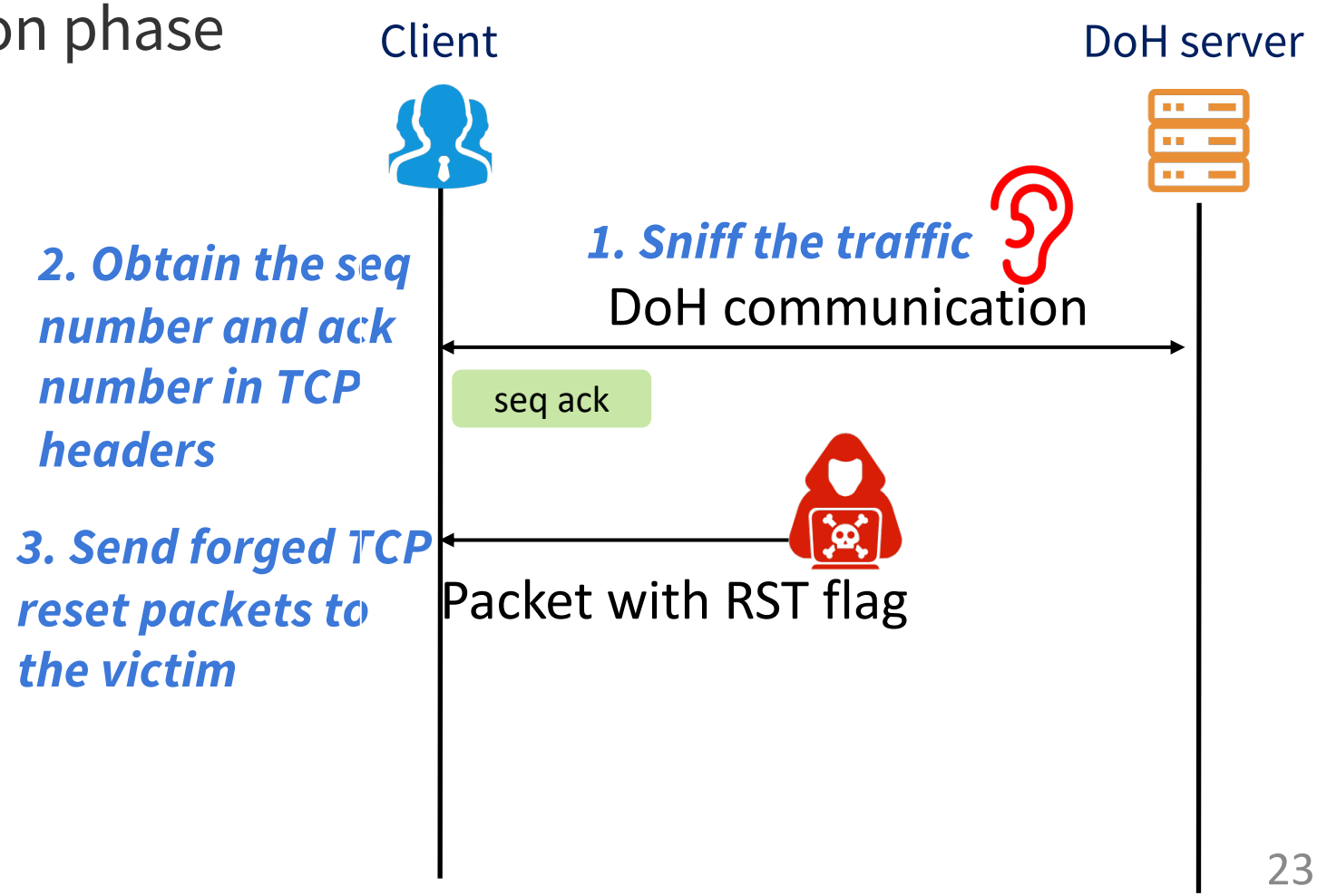
On-path Attacker



Downgrade Attack Method

- TCP Reset Attack
  - Target URI resolution phase

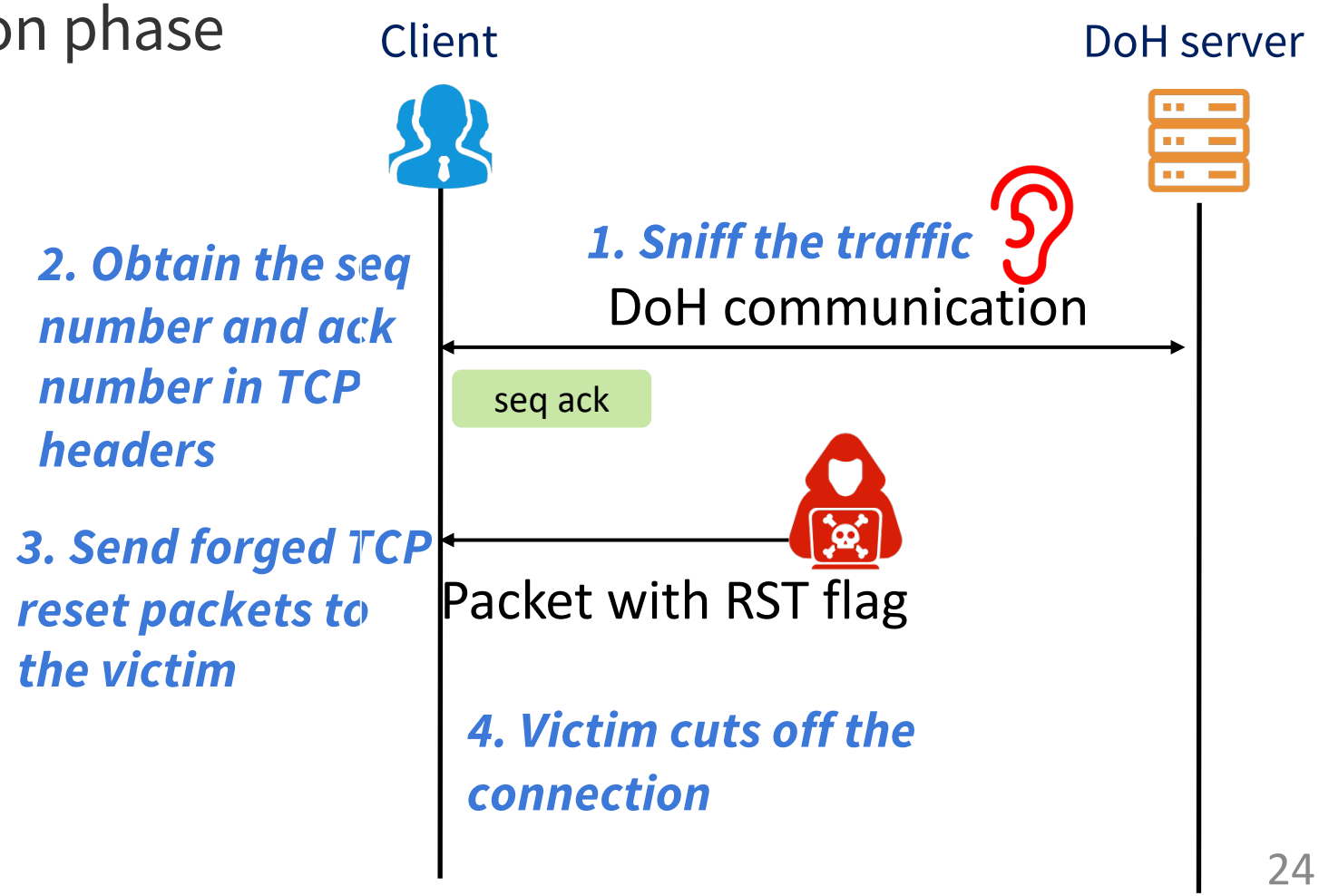
On-path Attacker



Downgrade Attack Method

- TCP Reset Attack
  - Target URI resolution phase

On-path Attacker



Measuring on Different Browsers

We examined 6 browsers with 4 attack vectors that are relevant to our attack model and found all combinations that lead to successful attacks.

Experimental Setup

- Evaluation Settings
  - Different Browsers ✕ different DoH servers ✕ different downgrade attacks
- Browser DoH Settings
  - Table 1 lists the detailed DoH set-tings of each browser.

Browser	Config	Profile	BType	Notif
Chrome 84.0.4147.89	OS&URI	Opportunistic*	Chrome+	No
Firefox 76.0.1	URI	Opportunistic*	Firefox	No
Edge 84.0.522.40	OS	Opportunistic	Chrome+	No
Brave 1.11.97	OS	Opportunistic	Chrome+	No
Opera 69.0.3686.77	URI	Opportunistic	Chrome+	No
Vivaldi 3.1.1929.458	OS	Opportunistic	Chrome+	No

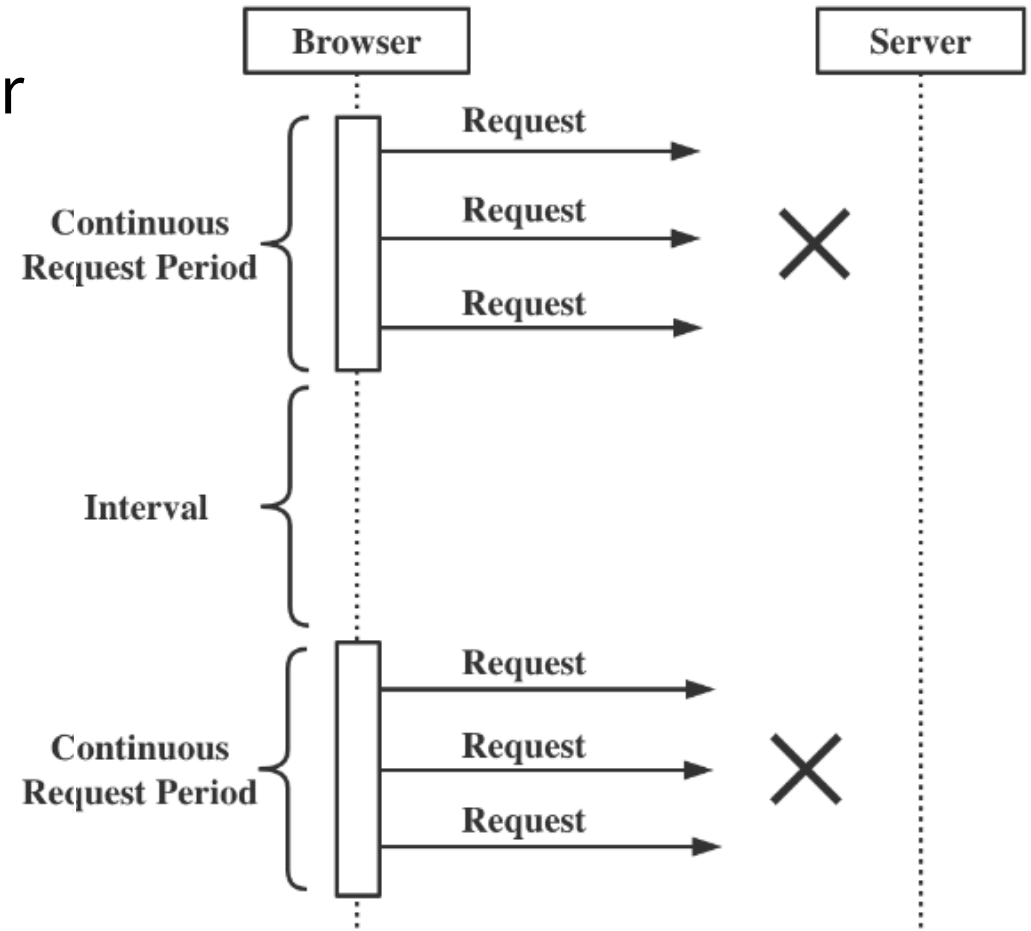
Table 1: Browser DoH settings

DoH Server	Domain name
Google	dns.google
Cloudflare	chrome.cloudflare-dns.com[1] cloudflare-dns.com
Quad9	dns.quad9.net
Umbrella/OpenDNS	doh.opendns.com
CleanBrowsing	doh.cleanbrowsing.org
Comcast	doh.xfinity.com
DNS.SB	doh.dns.sb

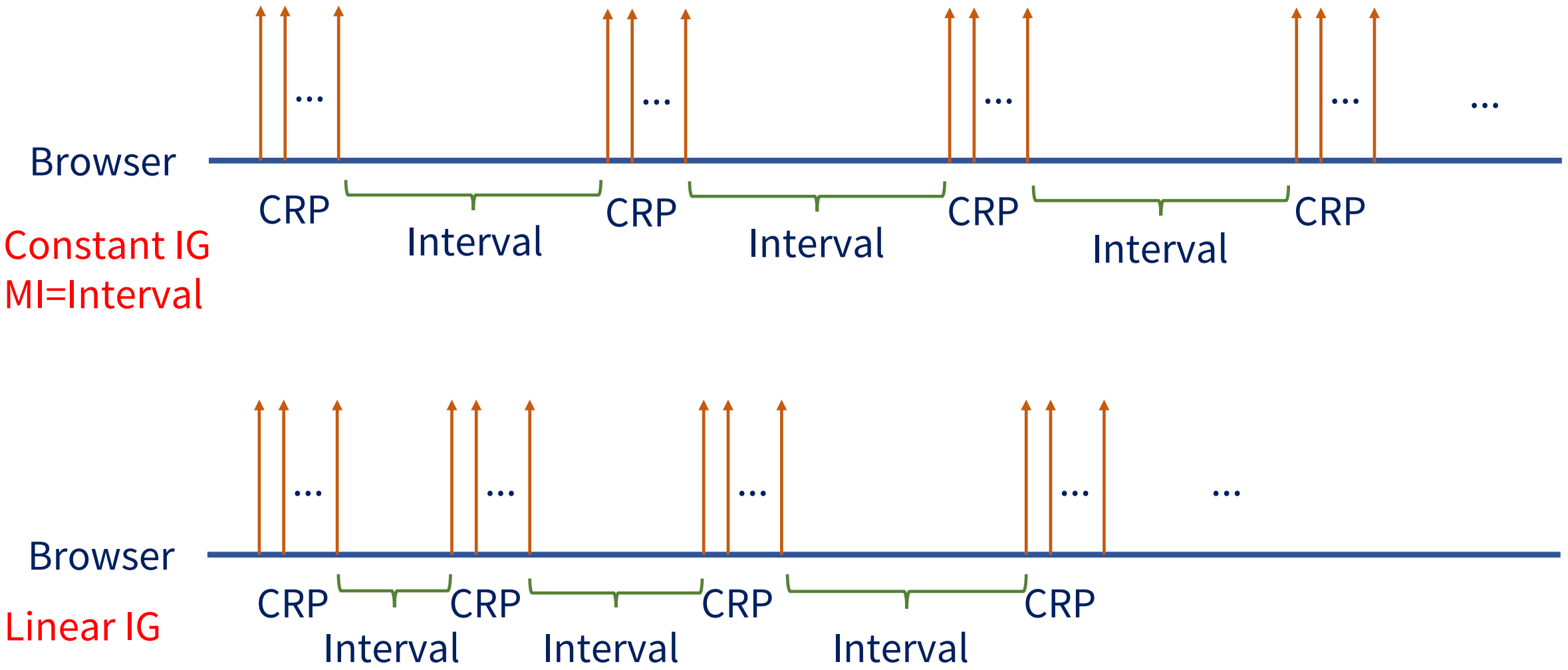
Table 2: Domain names of to DoH resolvers

Terminology

- Continuous Request Period (CRP)
  - When the connection fails, browser will keep trying to send reconnect requests within some period
- Interval Growth (IG)
  - The growth pattern of the interval
- Max Interval (MI)
  - The maximum value of interval as max interval



IG + MI


Browser
CRP
Interval
CRP
Interval
CRP
Interval
CRP
Constant IG
MI=Interval
Browser
CRP
Interval
CRP
Interval
CRP
Interval
CRP
Linear IG

Result

- Interesting Observation
  - Browser's response behavior will follow a pattern
  - None of the browsers prompt the user
  - The extra latency is not prominent when retrying DoH connection
  - Opportunistic profile enable by default
- Conclusion
  - Difficult for users to discover the attacks
  - Easy for attackers to implement the attacks

Attack	BType	CRP	IG	MI
DNS Spoofing	Chrome+	0.09	Linear	N/A
	Firefox	0.10	Constant	65.51
DNS Intercepting	Chrome+	36.52	Linear	N/A
	Firefox	15.01	Linear	50.50
TCP RST Injection	Chrome+	Random	Linear	N/A
	Firefox	Random	Linear	N/A
TCP Intercepting	Chrome+	10.98	Constant	63.84
	Firefox	0.27	Linear	65.25

Browser	Config	Profile	BType	Notif
Chrome 84.0.4147.89	OS&URI	Opportunistic*	Chrome+	No
Firefox 76.0.1	URI	Opportunistic*	Firefox	No
Edge 84.0.522.40	OS	Opportunistic	Chrome+	No
Brave 1.11.97	OS	Opportunistic	Chrome+	No
Opera 69.0.3686.77	URI	Opportunistic	Chrome+	No
Vivaldi 3.1.1929.458	OS	Opportunistic	Chrome+	No

Feedback after Disclosure

- Browser Vendors Response
  - None of the browsers will make a step to address our attacks
  - The user notification is deliberately ignored

- Analysis
  - Missing user notification is problematic
  - The integration of user notification into browser UI should incur moderate effort and overhead
  - Users should be put into the decision loop

The bar of downgrade attack is relatively low

Suggestion

- Revising DoH Implementations
  - Redesign DoH option UI
  - Support strict privacy profile
  - Enable user notification

- Revising DoH Protocols
  - Use IP address of DoH server instead of URI
  - Embed IP directly in URI template as the hostname

  Eg. https://dns.quad9.net/dns-query ---> https://9.9.9.9/dns-query

Summary

- We studied how browsers implement and configure DoH
- We perform the first study of downgrade attacks in a realistic lab environment
- We discuss the possible countermeasures at the implementation and protocol level