45th IEEE Symposium on Security and Privacy

DNSBomb: A New Practical-and-Powerful Pulsing DoS Attack Exploiting DNS Queries-and-Responses

Xiang Li, Dashuai Wu, Haixin Duan✉️, and Qi Li✉️

Presenter: **Xiang Li**, Tsinghua University

May 2024

@THU

Attack Impact

Our DNSBomb attack could be exploited to DoS arbitrary targets with pulsing traffic.

The bandwidth amplification factor could be >20,000x.

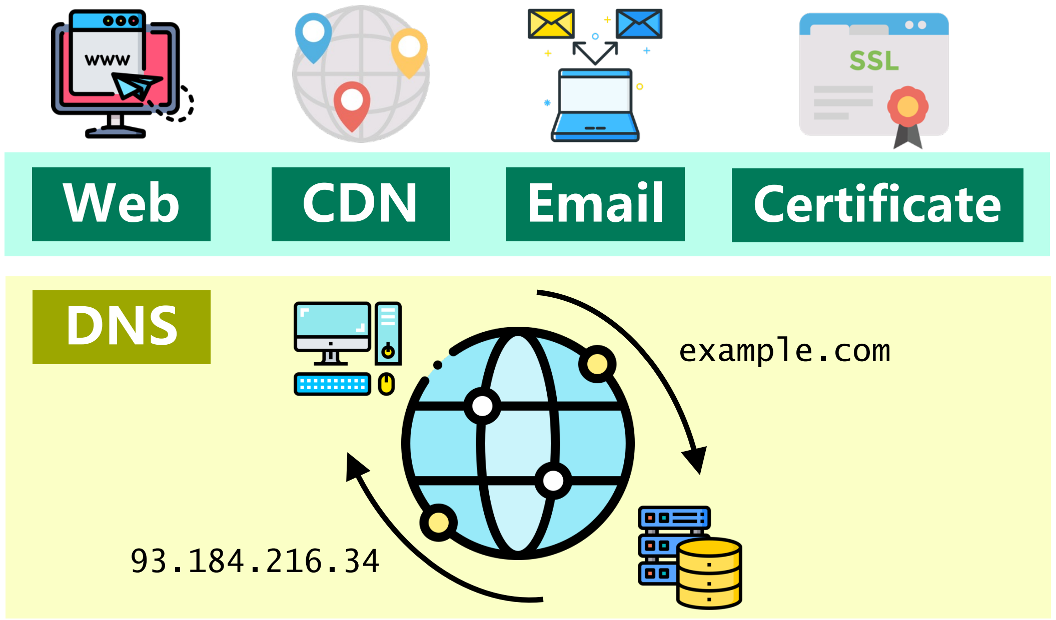
Domain Name System (DNS)

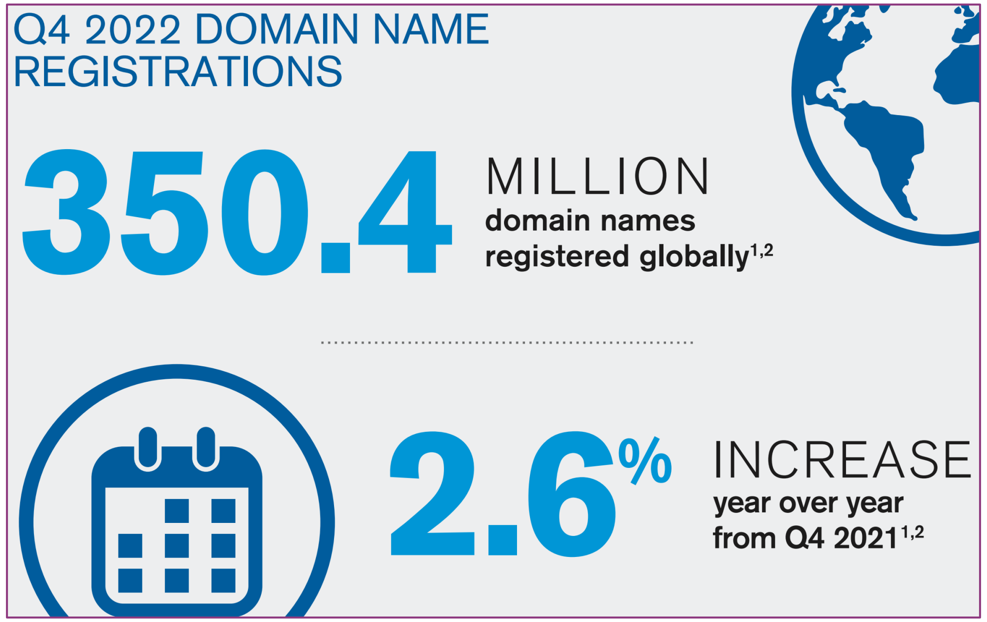
➢ DNS Overview

❑ Translating domain names to IP addresses

❑ Entry point of many Internet activities

❑ Domain names are widely registered

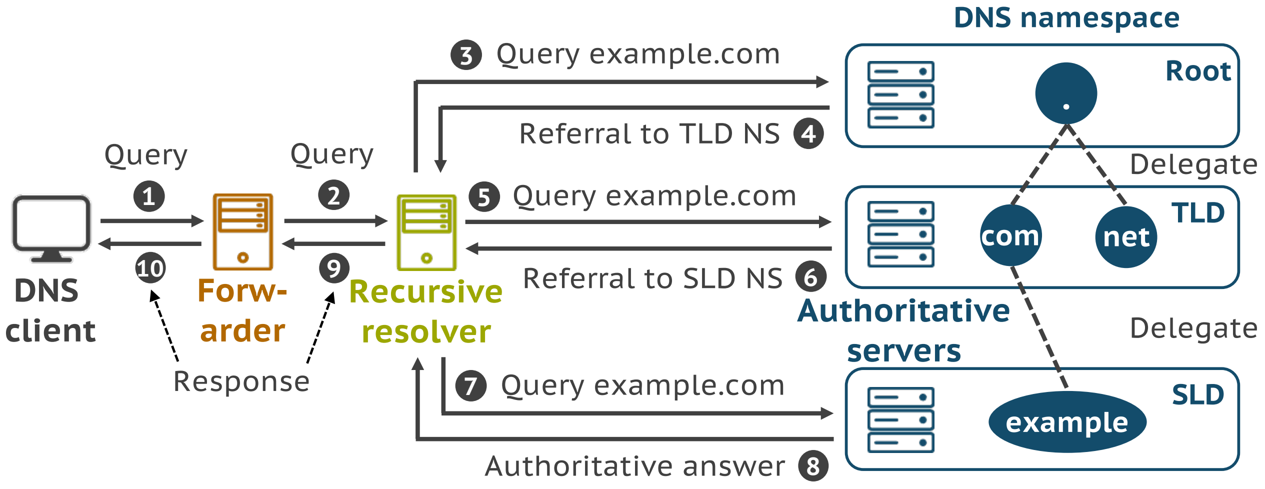




verisign.com/dnib

Domain Name System (DNS)

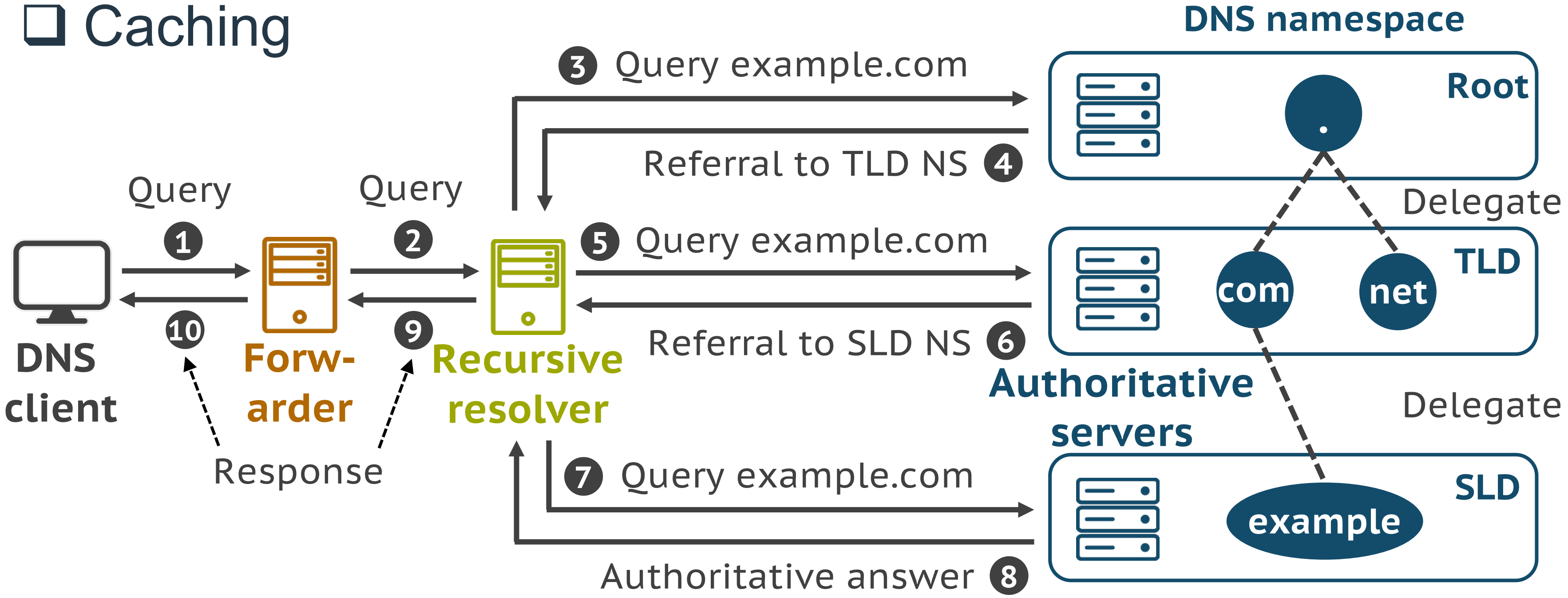
- **Hierarchical Name Space**
  - Authoritative zones: root, TLD, SLD → DNS records
  - Domain delegation → Domain registration
- **Multiple Resolver Roles**
  - Client, forwarder, recursive, authoritative
  - Caching
- **Iterative Resolution Process**
  - Client-server style



Domain Name System (DNS)

➢ DNS Resolution Process

- ❑ Primarily over UDP
- ❑ Iterative and recursive
- ❑ Caching



Query

SP=50000	DP=53	TXID=1001
QD	example.com A?	
AN	(empty)	
AU	(empty)	
AR	(empty)	

Response

SP=53	DP=50000	TXID=1001
QD	example.com A?	
AN	example.com A 1.1.1.1	
AU	(empty)	
AR	(empty)	

Takeaway

Since DNS is the cornerstone of the Internet, enabling multiple critical services and applications,

For a long time, attackers have been attempting to carry out **traffic amplification attacks** through DNS.

Question

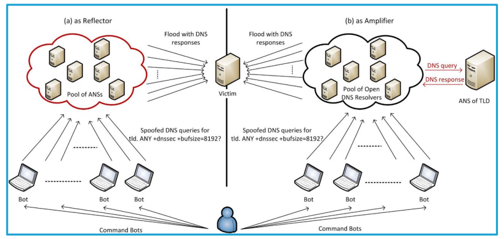
What is the DNS amplification attack?

Attackers exploit open DNS resolvers to flood a target with **an overwhelming amount of DNS traffic**.

DNS Amplification Attack

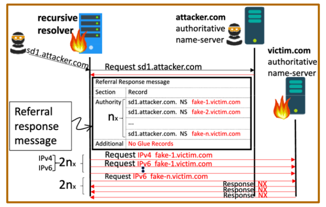
- **Target**
  - ❑ To flood a target with amount of DNS traffic
- **Taxonomy**
  - ❑ Bandwidth amplification attack
  - ❑ Packet amplification attack

2014



DNS reflection amplification attack by ANY/TXT/DNSSEC

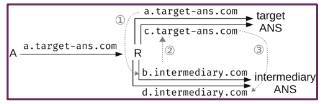
2018



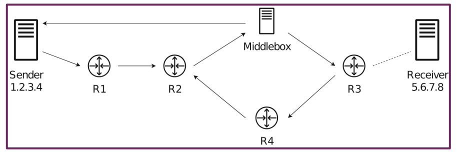
NXNSAttack

2020

DNS Unchained



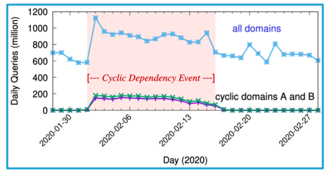
2021



Routing Loops as mega Amplifiers

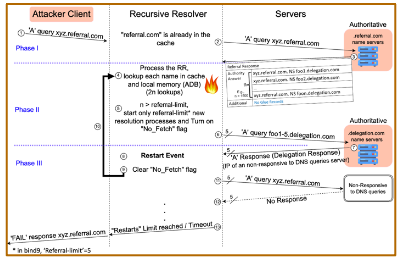
2022

TsuNAME

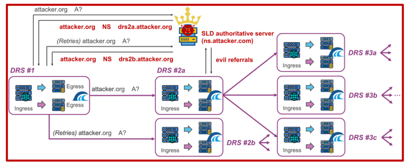


2023

NRDelegationAttack



2023



TsuKing

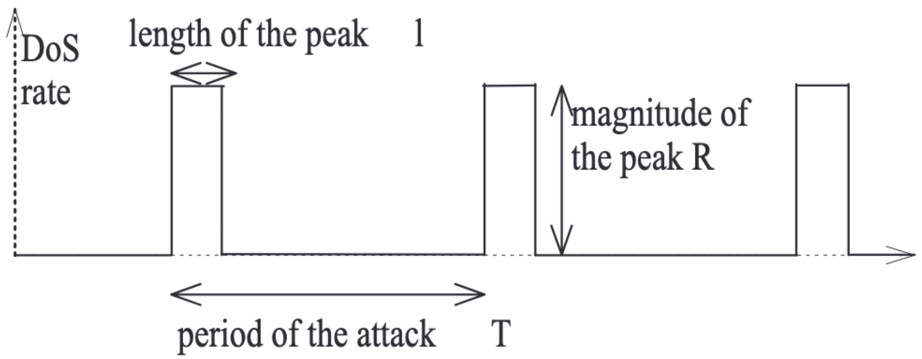
Takeaway

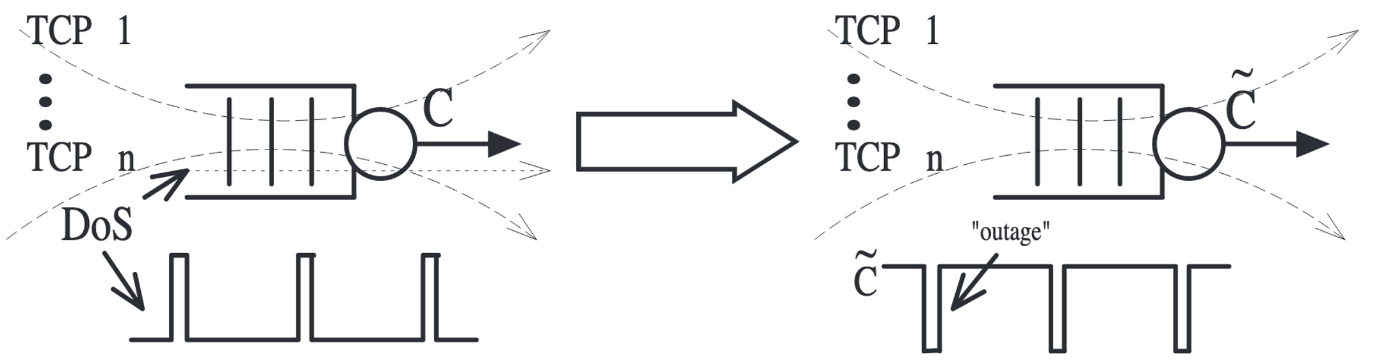
However, the traditional DNS amplification attack could be easily detected by the amount of traffic.

Researchers have proposed new amplification attacks with the **hard-to-detect pulsing DoS traffic**.

Pulsing DoS Attack (1/4)

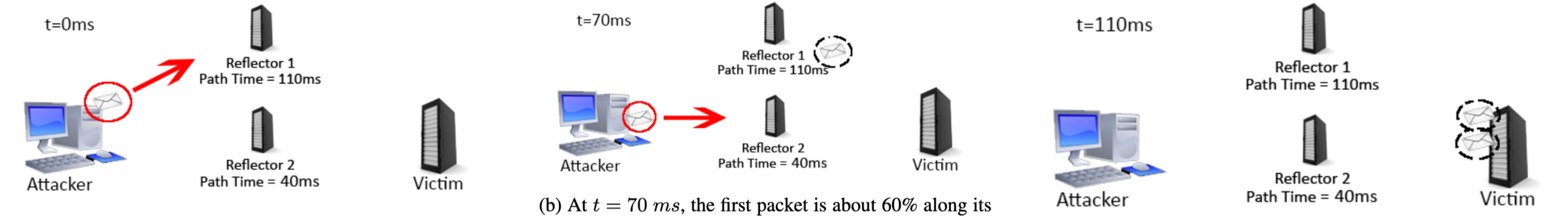
- **Originating from SIGCOMM '03#Shrew attack**
  - **A low-rate TCP-targeted DoS attack**
    - If the period of DoS flow approximating the RTO, pkts always losing
  - From 2003 - 2015, **various works targeting different scenarios**
    - Routing, VoIP, application servers, P2P, cloud, and others
    - But just in theory, **no work figuring out constructing pulsing traffic**





Pulsing DoS Attack (2/4)

- **Oakland '15#DNS-based Pulsing DoS Attack**
  - Using **latency** to **concentrate a low-rate flow** into a high-rate pulse
  - **Various open resolvers worldwide**
    - A wide range of paths and latencies
    - But, the latency is **at most 1s (800ms)**
  - Amplification factor: **10x**



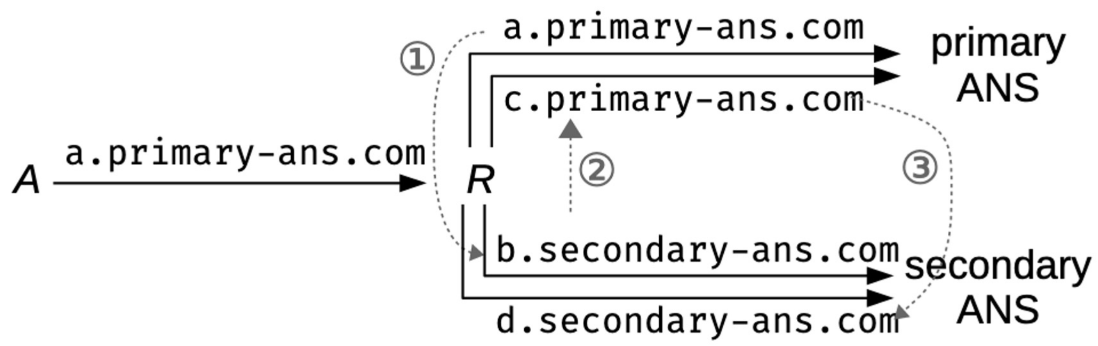
(a) At $t = 0\ ms$, the attacker sends one packet towards reflector 1

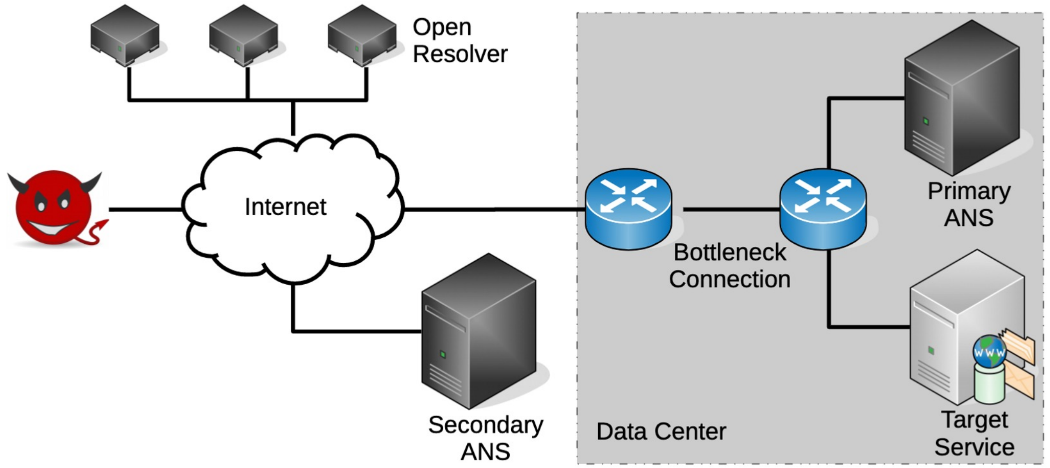
(b) At $t = 70\ ms$, the first packet is about 60% along its path to the victim and the attacker sends another packet to reflector 2

(c) At $t = 110\ ms$, both packets arrive at the victim

Pulsing DoS Attack (3/4)

- **Woot '18#DNS-based Pulsing DoS Attack**
  - Using **latency and CNAME-chaining** to **construct a high-rate pulse**
  - **More open resolvers worldwide**
    - A wide range of paths and latencies
  - **Attack the shared link: bottleneck**
  - Amplification factor: **10x**

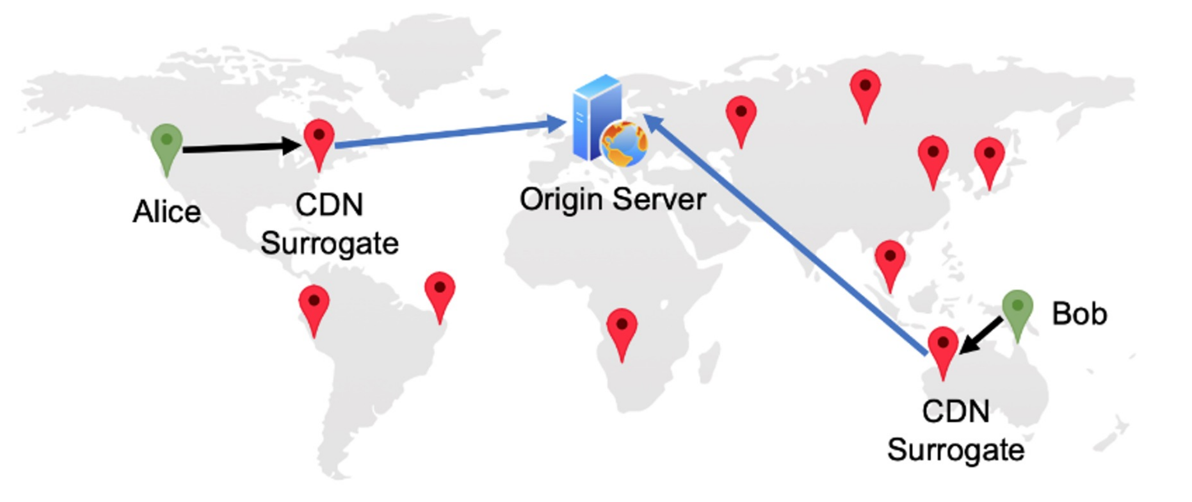


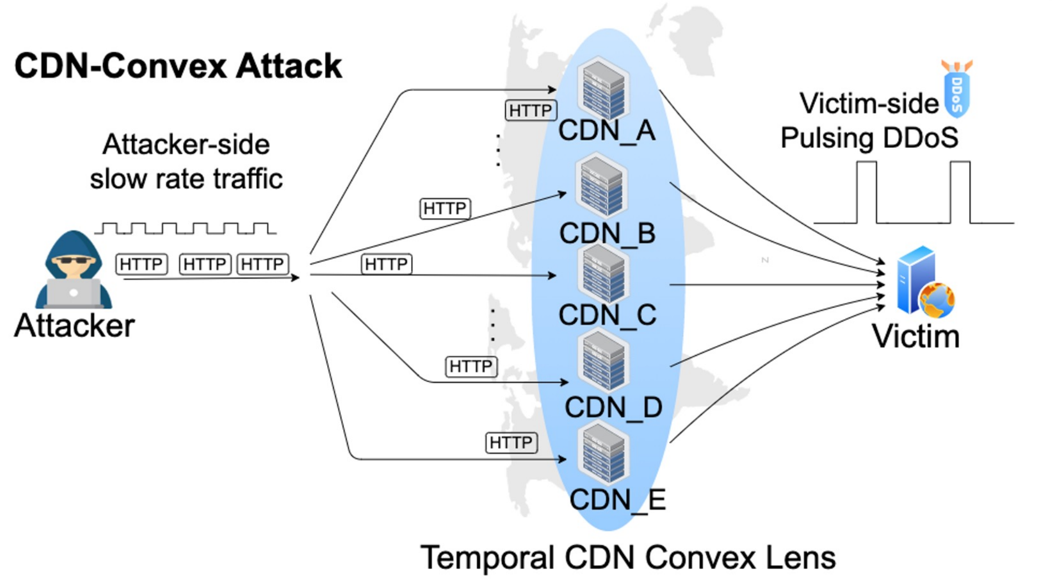


Pulsing DoS Attack (4/4)

➢ **Security '23#CDN-Assisted Pulsing DoS Attack**

- ❑ Using **CDN and HTTP (DNS)** to **construct a high-rate pulse**
- ❑ **Various CDN nodes worldwide**
- ❑ **Three ways: latency, CDN-chaining, and DNS-holding (fragment)**
- ❑ Amplification factor: **1,500+ (108+MBps)**

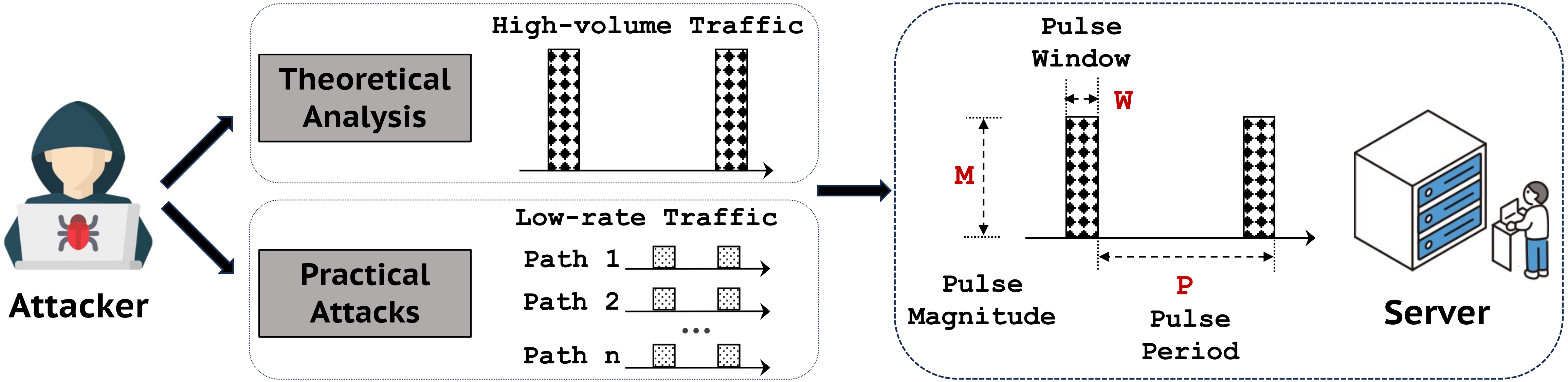




Pulsing DoS Attack

➢ Summary of Pulsing DoS Attack

- ❑ Concentrating a low-bandwidth traffic into a high-bandwidth pulsing
- ❑ **Cannot be detected by traditional IDS** (low-rate among a while)
- ❑ Impact is hugely causing pkts loss



Takeaway

However, previous pulsing DoS attacks could only yield a low amplification factor or require a large pulse period. (Not practical and powerful enough)

In this paper, we observe the capacity of DNS resolvers to **concentrate traffic has never been studied in depth**.

DNSBomb Attack

- ➢ **What is the DNSBomb attack**
  - ❑ Proposed by our **NISL** lab, published at **[IEEE S&P 2024]**
  - ❑ **A new practical and powerful DNS-based pulsing DoS attack**
    - o Concentrating a low-rate query traffic into a high-rate response pulsing
  - ❑ **Exploiting three inherent DNS mechanisms (defense) to DoS (attack)**
    - o **timeout**, **query aggregation**, and **response fast-returning**

Dragon Ball Kame Hame Ha (Blast wave)

① Kame (Starting) ② Hame (Gathering energy) ③ Ha (Releasing blast)

DNSBomb Attack

➢ Threat Model

❑ Step 1: Ka-me

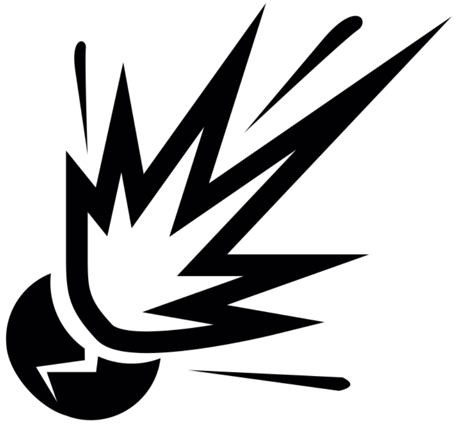
- Accumulating DNS Queries

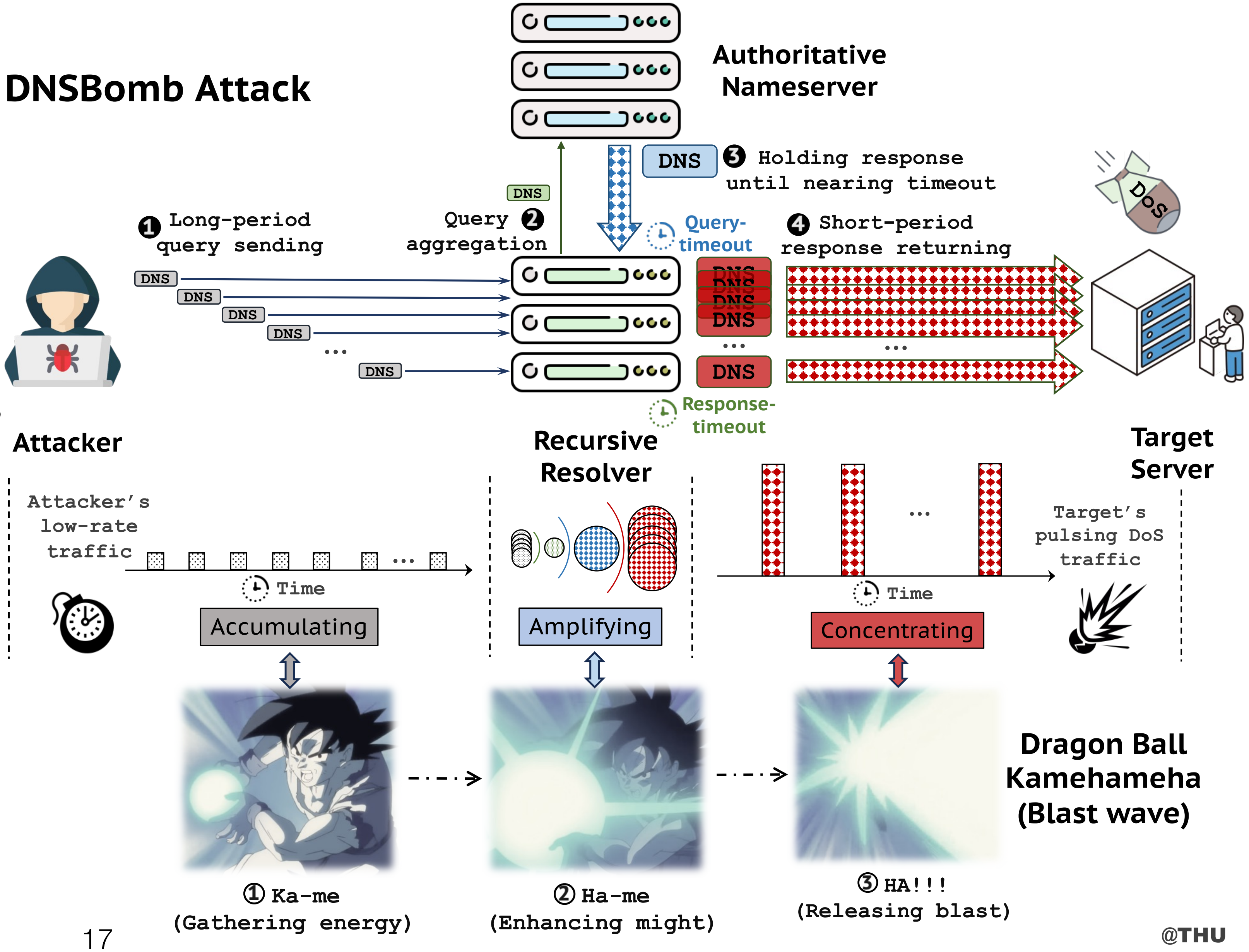
❑ Step 2: Ha-me

- Amplifying DNS Queries into Responses

❑ Step 3: HA!!!

- Concentrating DNS Responses





Three Inherent DNS Mechanisms (1/3)

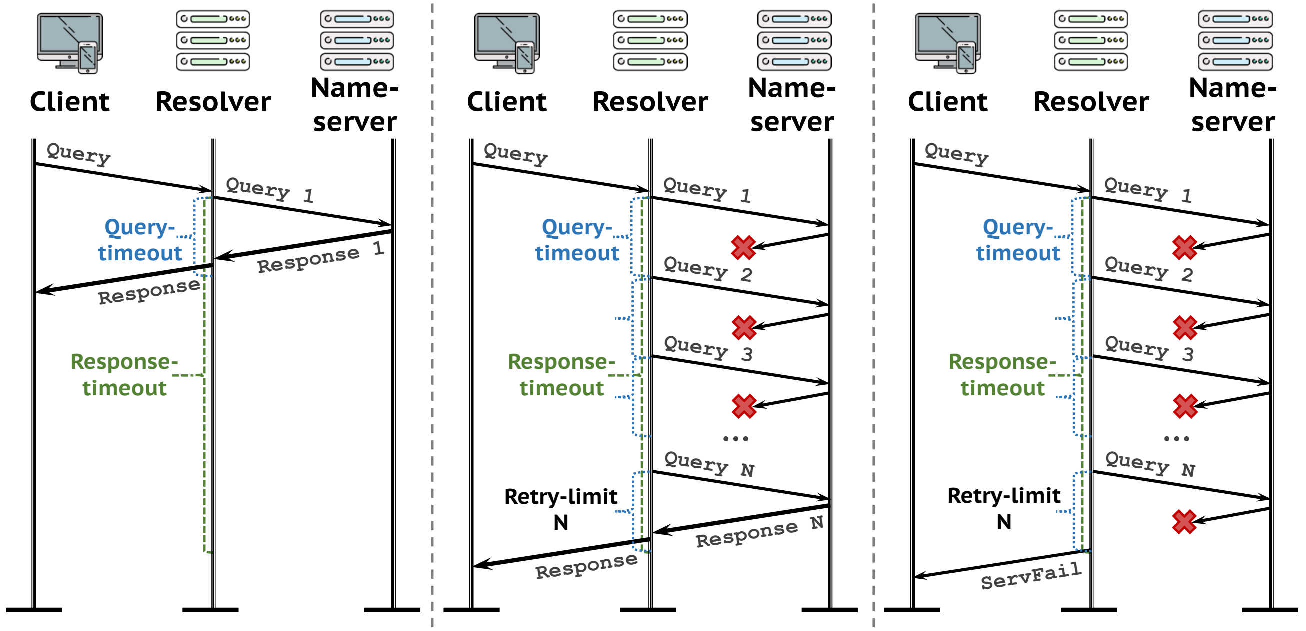
➢ **DNS Resolution Timeout**

❑ Waiting for responses from the auth. until timeout (**guaranteeing availability**)

- **Query timeout and response timeout, retry**

❑ **Attacker: accumulating large queries at a low sending-rate**

- during the timeout window

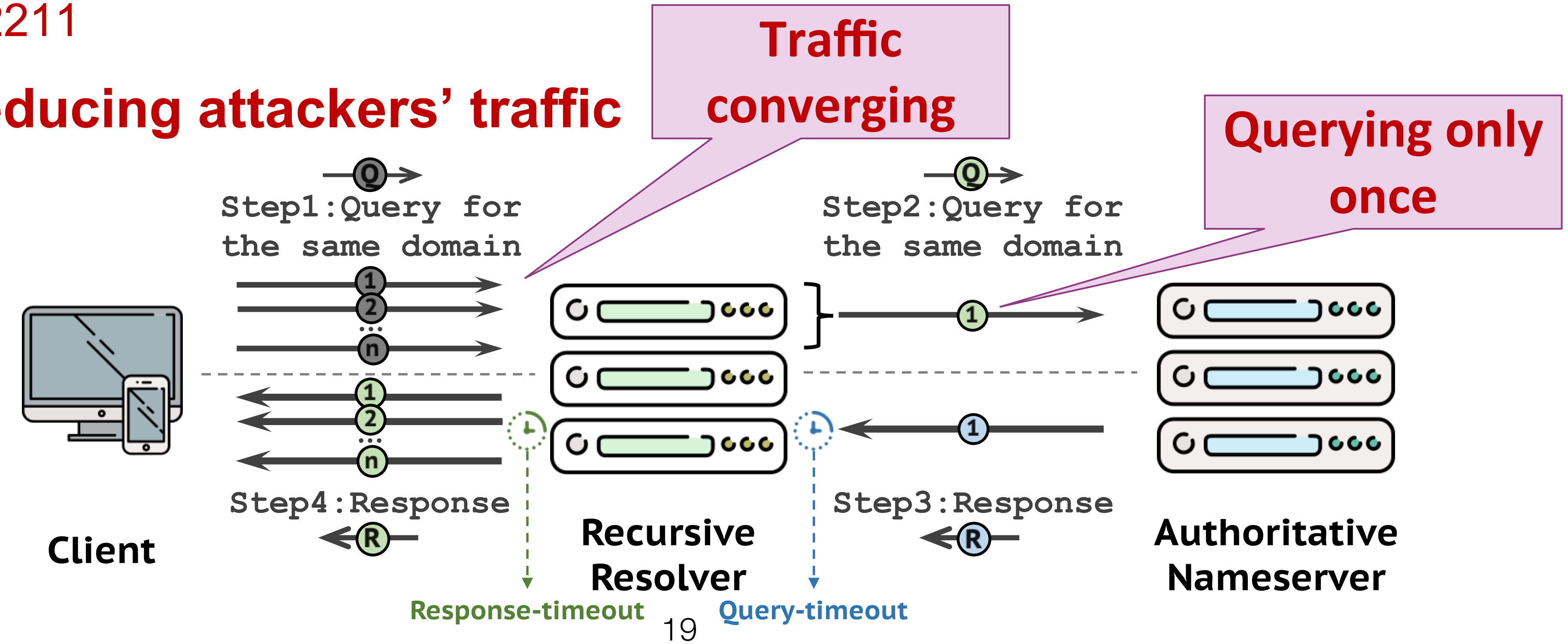


@THU

Three Inherent DNS Mechanisms (2/3)

➢ DNS Query Aggregation

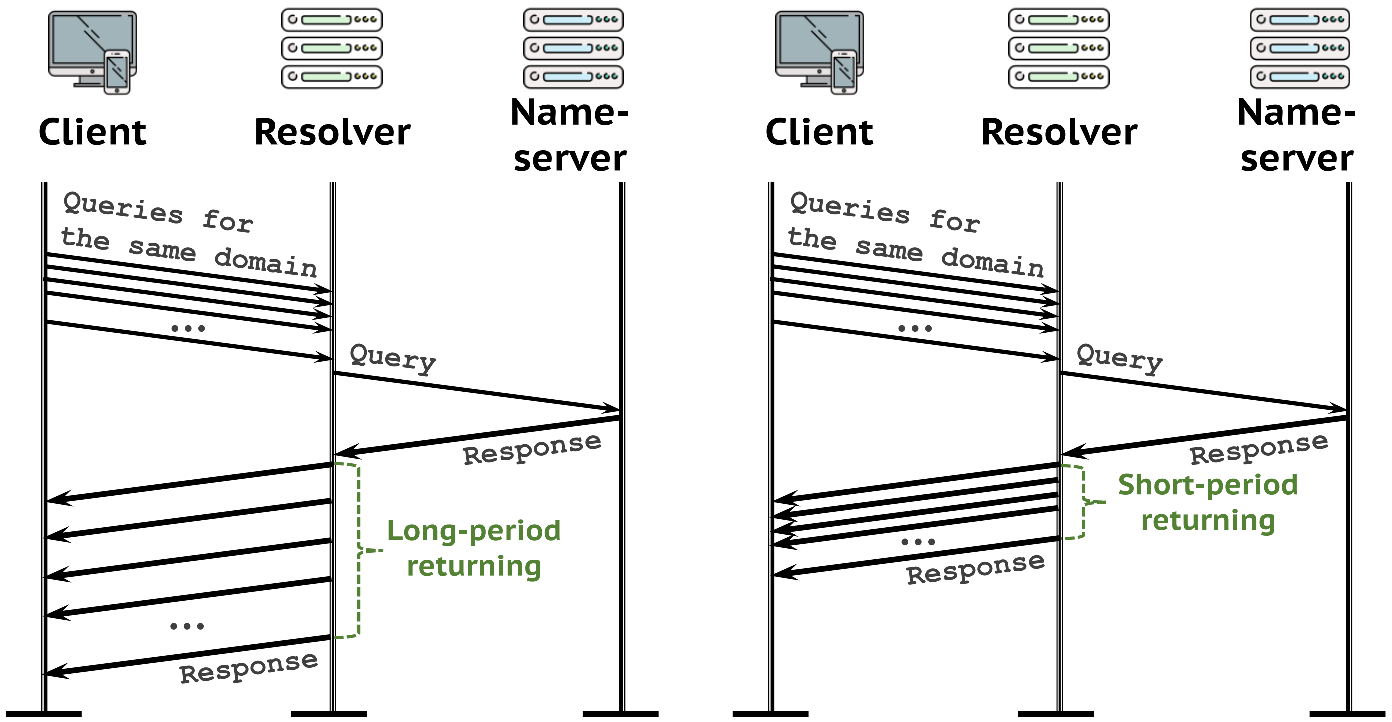
- ❑ Issuing one resolver-query for multiple simultaneous client-requests on the same domain name (**protecting security**)
- ❑ Defending against DNS birthday cache poisoning attack
  - o CVE-2002-2211
- ❑ **Attacker: reducing attackers' traffic**



Three Inherent DNS Mechanisms (3/3)

➢ DNS Response Fast-returning

- ❑ Returning responses to the client when receiving valid responses from the auth. (**enhancing reliability**)
- ❑ **Attacker: concentrating traffic into the victim fast**



Other Techniques

➢ Increasing the Packet Size

❑ Using EDNS0

```
## UDP Layer
;; Source Port; Destination Port: 53;
## DNS Layer
;; TXID; Flags: QR=0; RCODE: NoError
;; QUESTION SECTION:
example.com.  A
;; ANSWER SECTION: NULL
;; AUTHORITY SECTION: NULL
;; ADDITIONAL SECTION: EDNS0=4,096
;; DNS UDP MSG SIZE: ~100B
```

(a) Query with EDNS0.

```
## UDP Layer
;; Source Port: 53; Destination Port;
## DNS Layer
;; TXID; Flags: QR=1; RCODE: ServFail
;; QUESTION SECTION:
example.com.  A
;; ANSWER SECTION: NULL
;; AUTHORITY SECTION: NULL
;; ADDITIONAL SECTION: EDNS0=1,232
;; DNS UDP MSG SIZE: ~100B
```

(b) ServFail Response.

```
## UDP Layer
;; Source Port: 53; Destination Port;
## DNS Layer
;; TXID; Flags: QR=1; RCODE: NoError
;; QUESTION SECTION:
example.com.  A
;; ANSWER SECTION: NULL
example.com.  A     x.x.x.0
example.com.  A     x.x.x.1
example.com.  A     x.x.x.2
......
example.com.  A     x.x.x.n
;; AUTHORITY SECTION: NULL
;; ADDITIONAL SECTION: EDNS0=4,096
;; DNS UDP MSG SIZE: ~4,096B
```

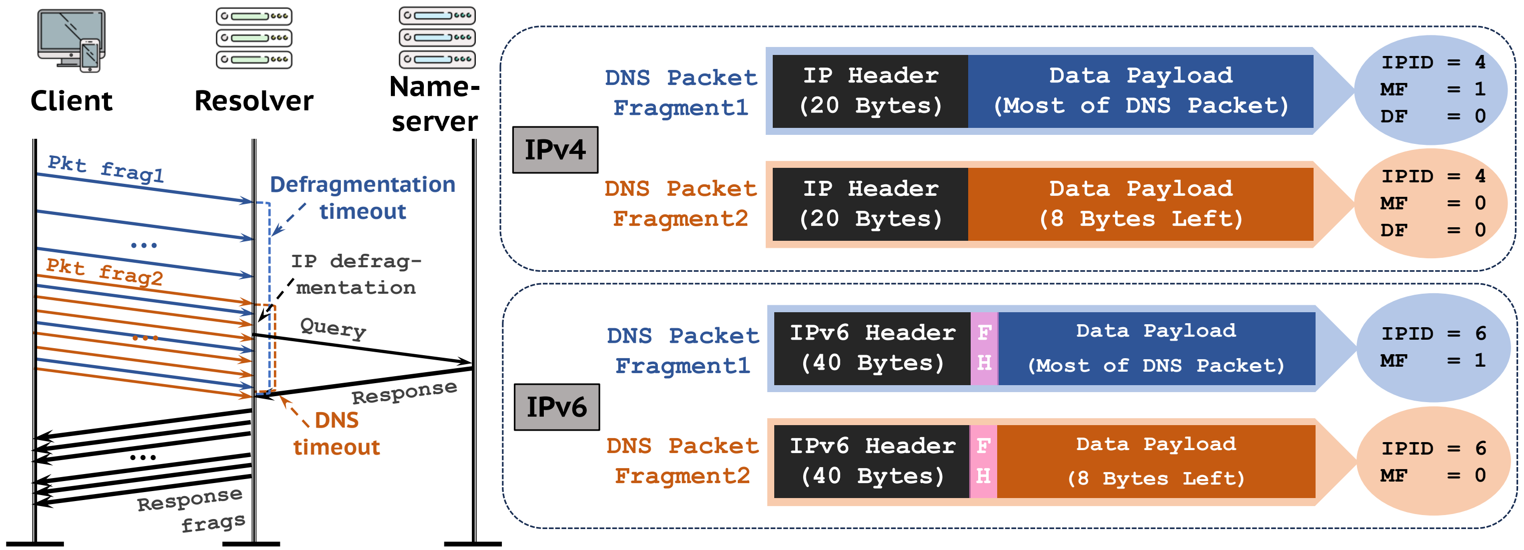
(c) Response with EDNS0.

```
......
example.com.  A     x.x.x.n
;; AUTHORITY SECTION: NULL
;; ADDITIONAL SECTION: NULL
;; DNS UDP MSG SIZE: <=512B
```

(d) Response without EDNS0.

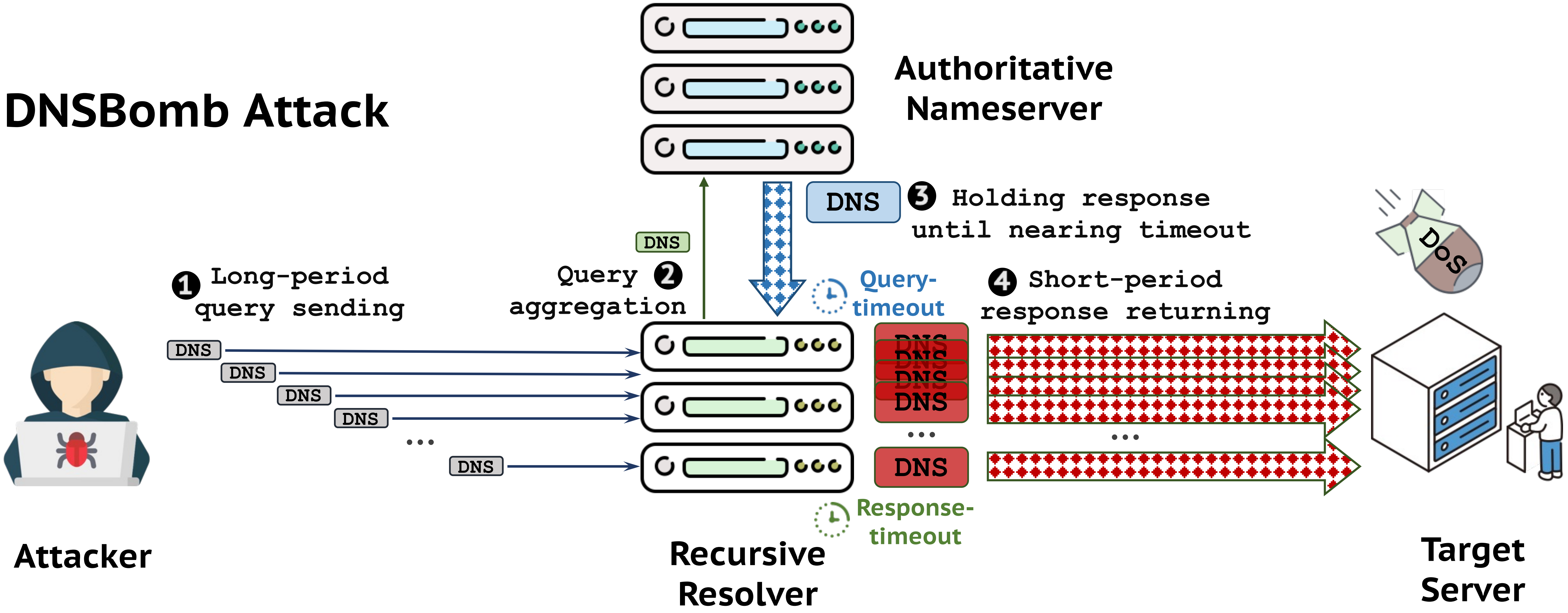
➢ Enlarging the Timeout Window

❑ Using defragmentation timeout



DNSBomb Attack

DNSBomb Attack

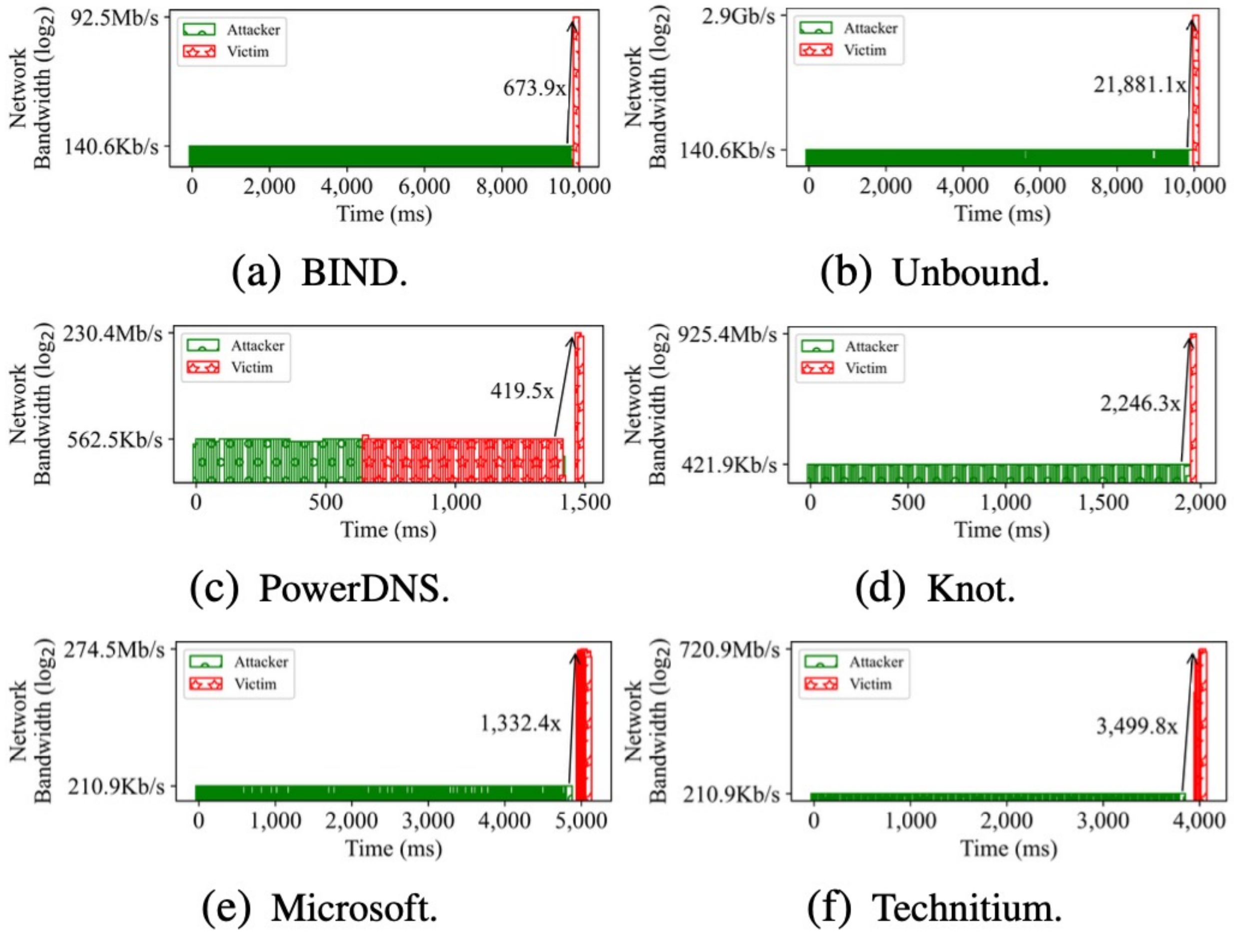


@THU

Vulnerable DNS Software

- **10 Mainstream DNS Software (All)**
  - Testing attack factors (timeout, pkt. size, returning-time) and local experiments

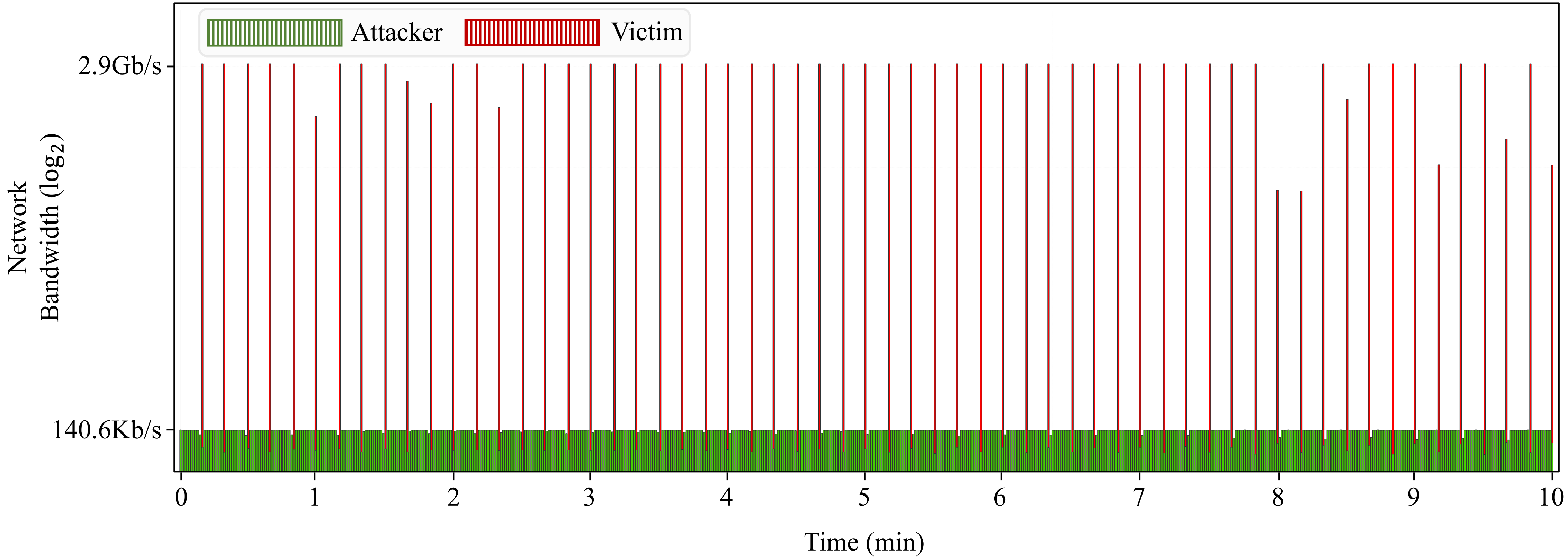
Software	Practical Attack Bandwidth			
	Attacker -side	Victim -side	Nameserver -side	BAF
BIND	140.6Kb/s	92.5Mb/s	155.5Kb/s	**673.9x**
Unbound	**140.6Kb/s**	**2.9Gb/s**	**140.6Kb/s**	**21,881.1x**
PowerDNS	562.5Kb/s	**230.4Mb/s**	70.3Kb/s	**419.5x**
Knot	421.9Kb/s	**925.4Mb/s**	70.3Kb/s	**2,246.3x**
Microsoft	210.9Kb/s	**274.5Mb/s**	70.3Kb/s	**1,332.4x**
Technitium	210.9Kb/s	**720.9Mb/s**	140.6Kb/s	**3,499.8x**
Simple DNS+	562.5Kb/s	36.4Mb/s	1,167.4Kb/s	66.3x
MaraDNS	140.6Kb/s	2.5Mb/s	123.4Kb/s	18.5x
Dnsmasq	140.6Kb/s	**458.9Mb/s**	210.9Kb/s	**3,341.8x**
CoreDNS	140.6Kb/s	**447.5Mb/s**	468.0Kb/s	**3,258.4x**



(a) BIND. (b) Unbound.
(c) PowerDNS. (d) Knot.
(e) Microsoft. (f) Technitium.

Long-term Experiments

- **Using Unbound**
  - Sending 1,000 queries in each round (10s) for 10m
  - **Results: stable**



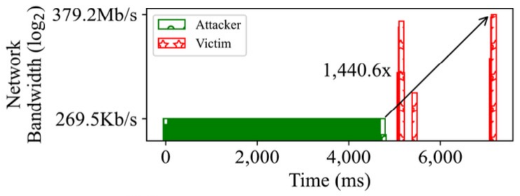
Experiments under Different Attack Factors

- **Multiple Resolvers x More Queries**
  - Unbound instances: 1-10
  - # of DNS queries: 1k-10k
  - **Results: more resolvers/queries → More victim-side traffic** (Gb/s)
  - The trend stops at 6k-8k because Unbound cannot concentrate more queries
  - The utmost bandwidth is 8.7Gb/s because our local network link is only 10Gb/s

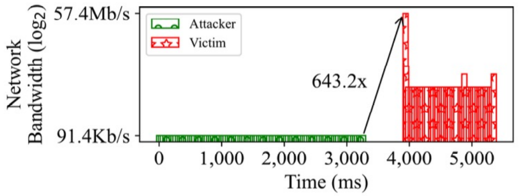
# of Unbound	# of DNS Queries									
	1k	2k	3k	4k	5k	6k	7k	8k	9k	10k
1	3.0	3.0	2.9	3.7	3.5	2.6	2.1	3.6	2.2	3.4
2	2.6	5.5	3.2	4.3	2.9	4.7	6.7	6.2	4.4	6.0
3	4.6	6.2	4.8	5.6	2.4	6.8	4.7	8.7	3.9	3.2
4	4.9	4.3	7.5	2.5	4.8	5.0	3.5	3.3	4.5	5.2
5	2.8	3.7	4.5	4.8	3.8	4.5	4.6	3.6	2.7	3.3
6	3.1	7.5	5.1	6.8	7.4	2.6	6.2	6.6	4.6	5.4
7	6.9	4.4	2.2	2.7	1.9	5.6	2.9	2.3	2.3	6.6
8	1.4	7.4	4.3	5.5	3.2	3.3	2.1	3.9	2.3	8.7
9	5.0	4.4	2.5	2.5	5.2	2.7	2.5	4.6	3.3	5.0
10	2.5	2.3	3.4	3.3	6.7	7.1	4.0	3.2	3.2	3.3

Vulnerable Public DNS Services

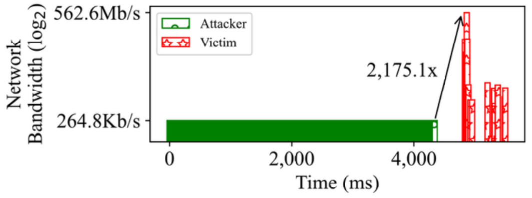
- **46 Public DNS Services (All)**
  - Testing their attack factors (timeout, pkt size, returning-time) and small experiments, **14/46:** BAF >1,000x



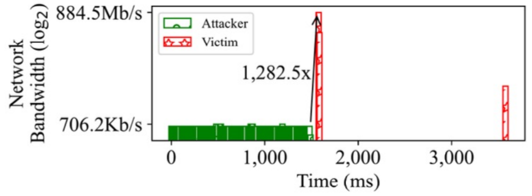
(b) 360 Secure DNS.



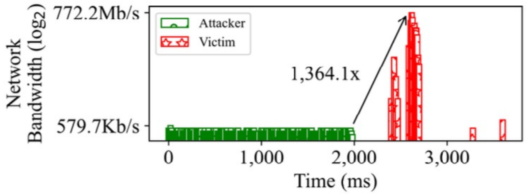
(c) Adguard DNS.



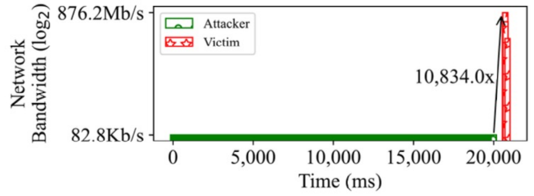
(m) Cisco OpenDNS.



(p) CloudFlare DNS.



(af) Level3 DNS.



(av) Yandex DNS.

Part Vendors	Practical Attack Bandwidth			
	Attacker -side	Victim -side	Nameserver -side	BAF
360 Secure DNS	269.5Kb/s	379.2Mb/s	269.5Kb/s	1,440.0x
AdGuard DNS	393.8Kb/s	699.5Mb/s	756.2Kb/s	1,819.0x
CIRA Shield DNS	264.8Kb/s	904.9Mb/s	165.6Kb/s	3,498.8x
Cisco OpenDNS	264.8Kb/s	562.6Mb/s	529.7Kb/s	2,175.1x
CloudFlare DNS	706.2Kb/s	884.5Mb/s	441.4Kb/s	1,282.5x
DNS.WATCH	248.4Kb/s	638.6Mb/s	540.6Kb/s	2,632.1x
DNSPod Public DNS	331.2Kb/s	398.3Mb/s	274.2Kb/s	1,231.1x
Dyn DNS	362.5Kb/s	383.1Mb/s	271.9Kb/s	1,082.2x
Level3 DNS	579.7Kb/s	772.2Mb/s	283.6Kb/s	1,364.1x
Neustar UltraDNS	248.4Kb/s	261.1Mb/s	689.1Kb/s	1,076.1x
Verisign Public DNS	248.4Kb/s	329.4Mb/s	459.4Kb/s	1,357.6x
Yandex DNS	82.8Kb/s	876.2Mb/s	536.7Kb/s	**10,834.0x**

Vulnerable Open Resolvers

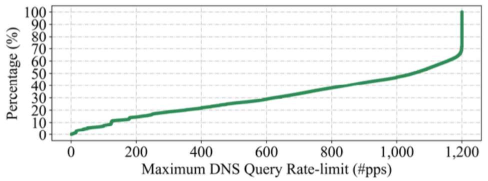
➢ Internet Scanning

- ❑ Designed probing policies
- ❑ Using XMap + fpdns
  - ○ Software identified: **517,075 (28.7%)**

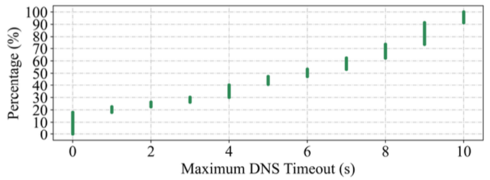
Type	Resolver number and percentage	
Collected	Alive on 07/05/2023	**1,801,275 (100.0%)**
Software identified	Microsoft DNS	143,928 (8.0%)
	Dnsmasq	96,331 (5.3%)
	BIND	44,016 (2.4%)
	Unbound	15,645 (0.9%)
	PowerDNS	6,367 (0.4%)
	Simple DNS+	166 (0.0%)
	Knot	2 (0.0%)

➢ Internet Measurement

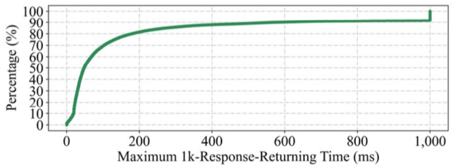
- ❑ Measuring attack factors, e.g.,
  - ○ **>50%** resolvers could accumulate >1k queries
  - ○ **>80%** resolvers support timeout of >1s
  - ○ **>60%** resolvers support pkt size of >1,232B



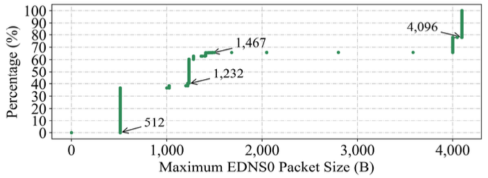
(a) Max. Rate-limit. Rate-limit Values > 1,200 are Shown as 1,200.



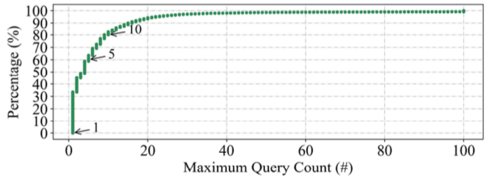
(b) Max. DNS Timeout. Timeout Values > 10s are Shown as 10s.



(e) Max. 1k-Responses-Returning Time. Time Values > 1s are Shown as 1s.



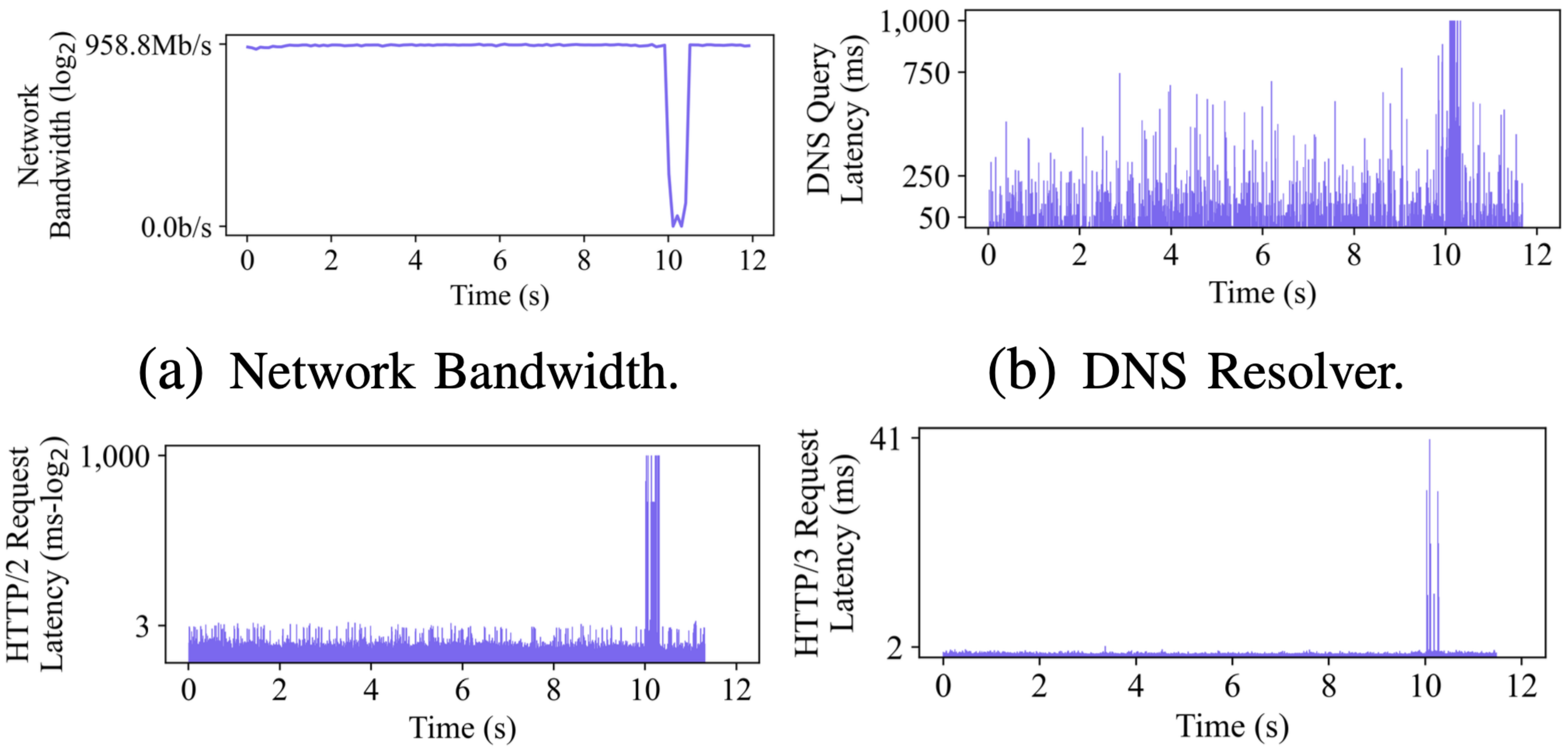
(c) Max. EDNS0 Packet Size. Size values > 4,096 are Shown as 4,096.



(d) Max. Query Count. Count Values > 100 are Shown as 100.

Evaluation of DNSBomb

- **Using Unbound**
  - Sending 10k queries within a timeout window of 10s
  - Attacking **a DNS resolver, HTTP/2 website, and HTTP/3 website**
    - **Network bandwidth is totally occupied**
    - **Resolver never received a query**
    - **HTTP/2 service cannot be fetched**
    - **HTTP/3 is not much affected**



(a) Network Bandwidth. (b) DNS Resolver.
(c) HTTP/2-based Website. (d) HTTP/3-based Website.

Mitigation Solutions

- **Limiting Attack Factors**
  - **6 experiments:** base, restricting **timeout** to 1s, **rate-limit** to 100, **pkt. size** to 1,232, **response-returning time** to 1s, all restrictions
  - **Best mitigation:** restricting the timeout and response-returning speed

Software	Base[1]		Timeout[2]		Rate-limit[3]		Pkt. Size[4]		Res. Time[5]		All[6]	
	BAF	*%*	*BAF*	*%*	*BAF*	*%*	*BAF*	*%*	*BAF*	*%*	*BAF*	*%*
BIND	673.9x	100.0%	122.5x	18.2%	1,347.8x	200.0%	673.9x	100.0%	13.5x	2.0%	47.2x	7.0%
Unbound	21,881.1x	100.0%	2,398.5x	11.0%	4,525.6x	20.7%	4,400.5x	20.1%	45.3x	0.2%	20.2x	0.1%
PowerDNS	419.5x	100.0%	178.9x	42.6%	1,132.1x	269.9%	237.6x	56.6%	257.8x	61.4%	20.2x	4.8%
Knot	2,246.3x	100.0%	1,225.3x	54.5%	1,347.8x	60.0%	2,246.3x	100.0%	40.4x	1.8%	13.5x	0.6%
Microsoft	1,332.4x	100.0%	280.7x	21.1%	2,649.8x	198.9%	700.8x	52.6%	44.9x	3.4%	20.2x	1.5%
Technitium	3,499.8x	100.0%	2,867.6x	81.9%	4,525.6x	129.3%	4,492.6x	128.4%	467.6x	13.4%	74.1x	2.1%
Simple DNS+	66.3x	100.0%	61.7x	93.0%	726.3x	1094.8%	97.7x	147.3%	17.5x	26.3%	20.2x	30.5%
MaraDNS	18.5x	100.0%	3.1x	16.7%	37.0x	200.0%	18.5x	100.0%	18.5x	100.0%	18.5x	100.0%
Dnsmasq	3,341.8x	100.0%	624.1x	18.7%	4,546.7x	136.1%	1,033.5x	30.9%	2,728.0x	81.6%	20.5x	0.6%
CoreDNS	3,258.4x	100.0%	524.2x	16.1%	4,389.8x	134.7%	821.8x	25.2%	158.4x	4.9%	20.5x	0.6%

[1]: Base Experiment. [2]: Timeout to 1s. [3]: Rate-limit to 100. [4]: Packet Size to 1,232. [5]: Response-Returning Time to Timeout. [6]: All Restrictions Set.

Vulnerability Disclosure

- All DNS Implementation are Vulnerable
  - Reporting to 10 DNS software and 46 vendors
  - 24 Discussed/Confirmed (10 CVEs)
- Industry-wide CVE-2024-33655

BIND 9 unbound
POWERDNS KNOT RESOLVER
Technitium Dnsmasq CoreDNS

114DNS 360安全DNS Akamai Vantio DNS CZ.NIC ODVR
DNS.SB TOM OneDNS quad9 SAFEDNS
ADGUARD DNS AliDNS 公共解析服务 Baidu DNS ByteDance DNS
CFIEC Public DNS CONTROL D DYN Yandex DNS

@THU

Wrap-up

Thanks for listening!
Any question?

Paper

Xiang Li, Tsinghua University
x-l19@mails.tsinghua.edu.cn

Tool