MMLAB Main Seminar

Silence is not Golden: Disrupting the Load Balancing of Authoritative DNS Servers

Fenglu Zhang (Tsinghua University), et al

Distinguished Paper Award
CCS'23 (November 26-30, 2023)

Hyunsoo Kim (hskim@mmlab.snu.ac.kr)

2024. 06. 13

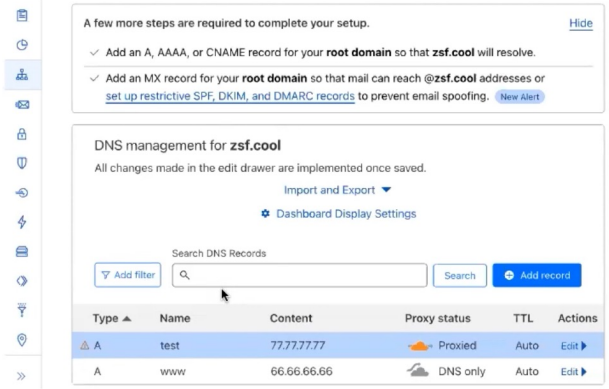
서울대학교 SEOUL NATIONAL UNIVERSITY

mmlab Network Convergence & Security Lab

Current Trends

- Domain hosting in cloud services
  - Cloud services provide the infrastructure to resolve the DNS query for hosted domains
  - They also provide user-friendly UI to help manage hosted domain
- As a result, numerous domains are sharing authoritative nameservers and load balancing is critical to the stability and security of domain hosting service

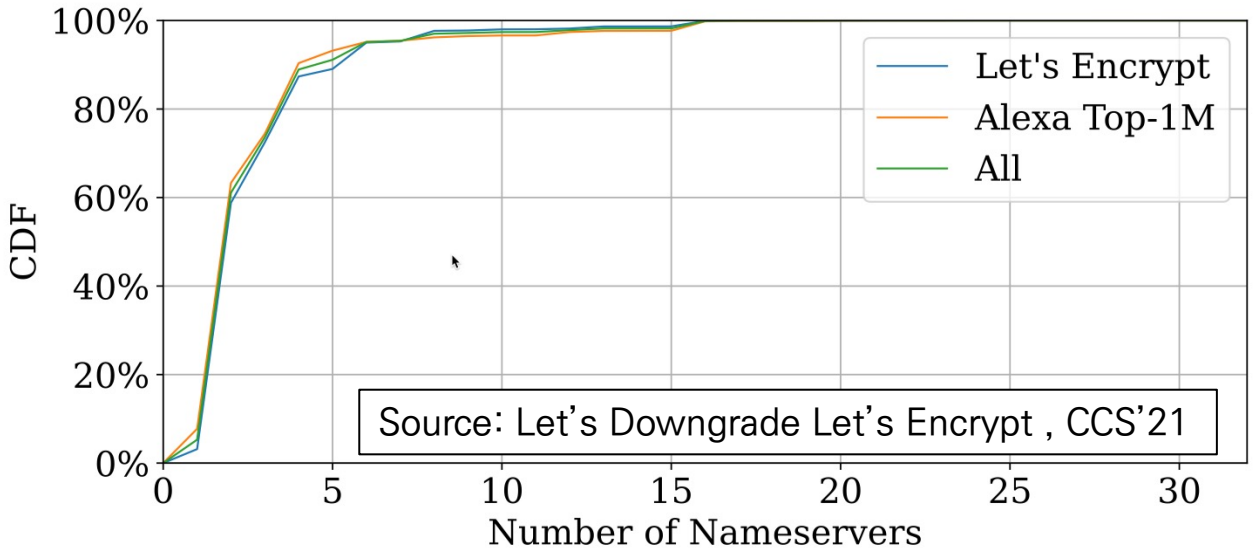
Some vendors of DNS hosting services



The user-friendly UI provided by a DNS hosting service

Built-in Load Balancing in DNS

- [RFC 1034] Domain Name Systems, 1987
  - By administrative fiat, we REQUIRE every zone to be available on at least two servers, and many zones have more redundancy than that
- [RFC 2182] Selection and Operation of Secondary DNS Servers, 1997
  - Secondary servers (Authoritative servers) MUST be placed at both topologically and geographically dispersed locations on the Internet



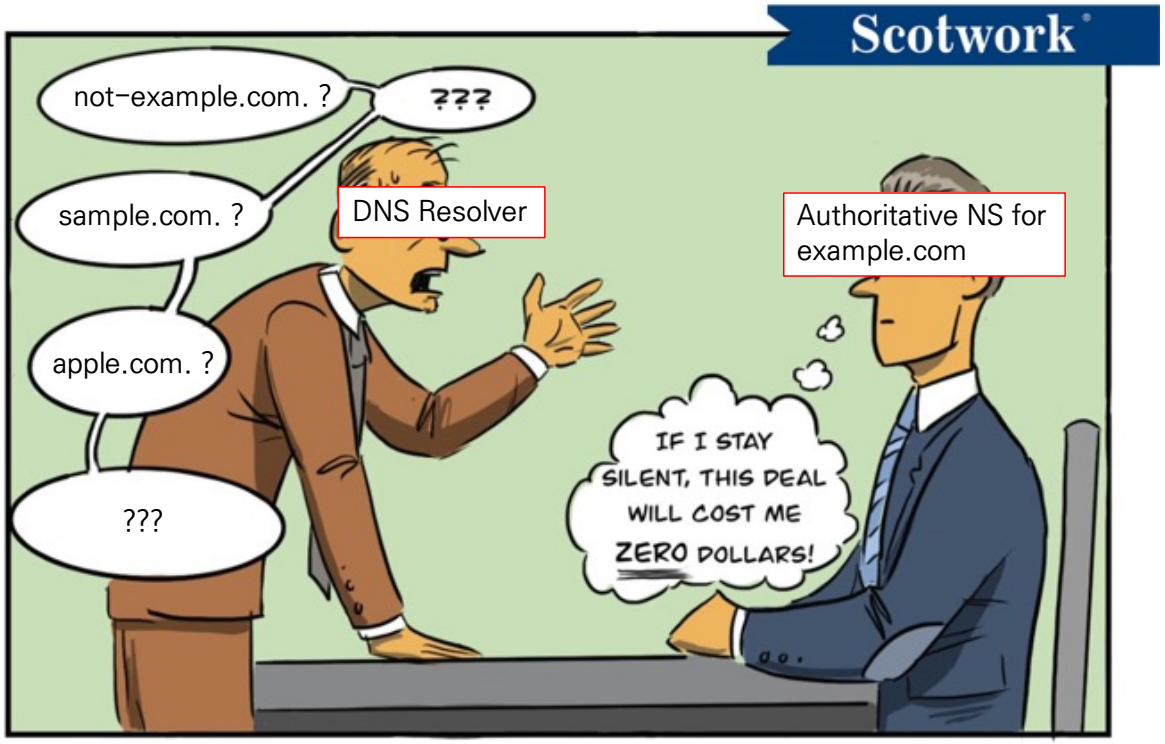
Security Impacts of Disrupting DNS Load Balancing

- **Bypassing defense mechanisms and overloading nameservers**
  - Redirecting legitimate DNS traffic to a specified target and no malicious traffic can be filtered
  - Bypassing defense mechanisms against traditional DoS attacks
- **Lowering the bar of traffic hijacking and cache poisoning**
  - Eliminating the possibility for clients to query diverse nameservers
  - DNS manipulation becomes less challenging since a unique path is dedicated to victims
- ***Let's Downgrade Let's Encrypt***
  - Reducing the number of reachable NSs to one during domain validation

  ➔ The attacker can obtain fraudulent certificate by BGP hijacking

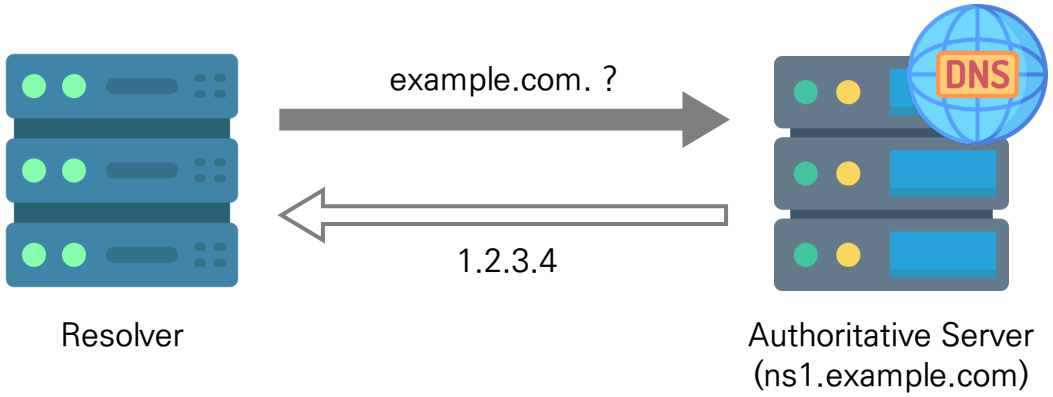
Misconfiguration of Authoritative Servers

- "Silence is Golden" strategy
- Extensive authoritative servers are configured to not respond to DNS requests which are outside of their authority



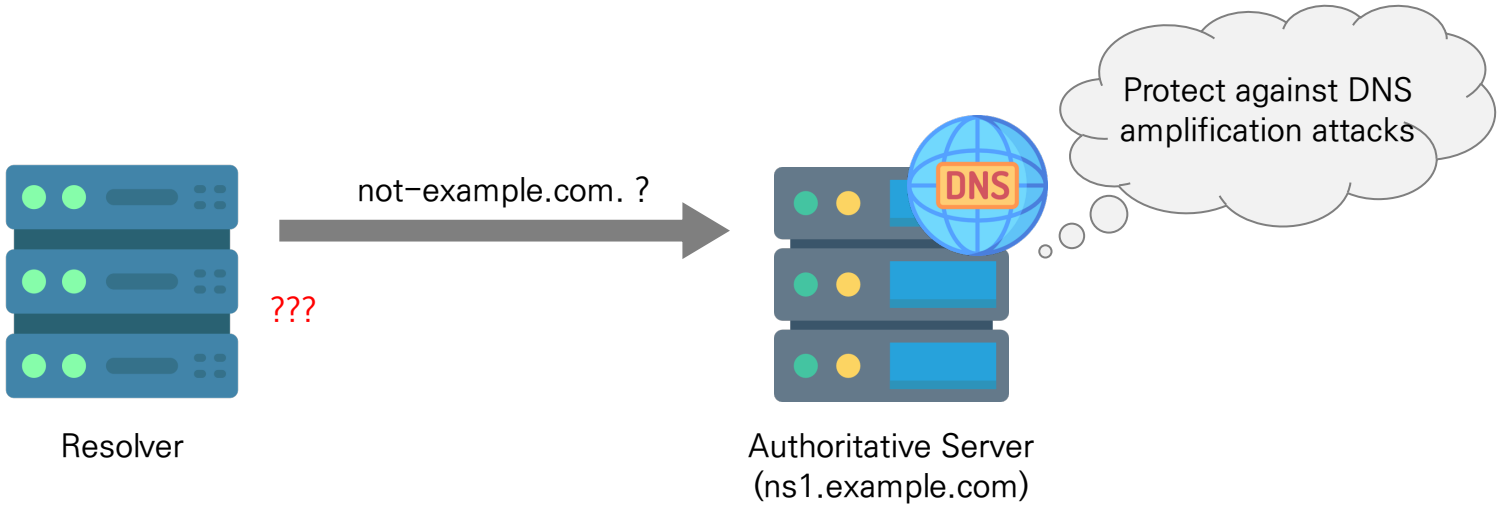
Misconfiguration of Authoritative Servers

- "Silence is Golden" strategy
- Extensive authoritative servers are configured to not respond to DNS requests which are outside of their authority



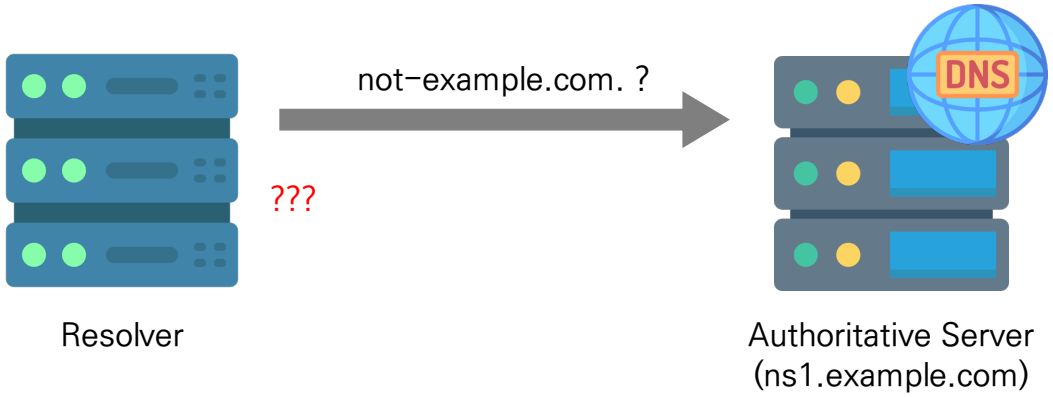
Misconfiguration of Authoritative Servers

- "Silence is Golden" strategy
- Extensive authoritative servers are configured to not respond to DNS requests which are outside of their authority



Misconfiguration of Authoritative Servers

- "Silence is Golden" strategy
- Extensive authoritative servers are configured to not respond to DNS requests which are outside of their authority

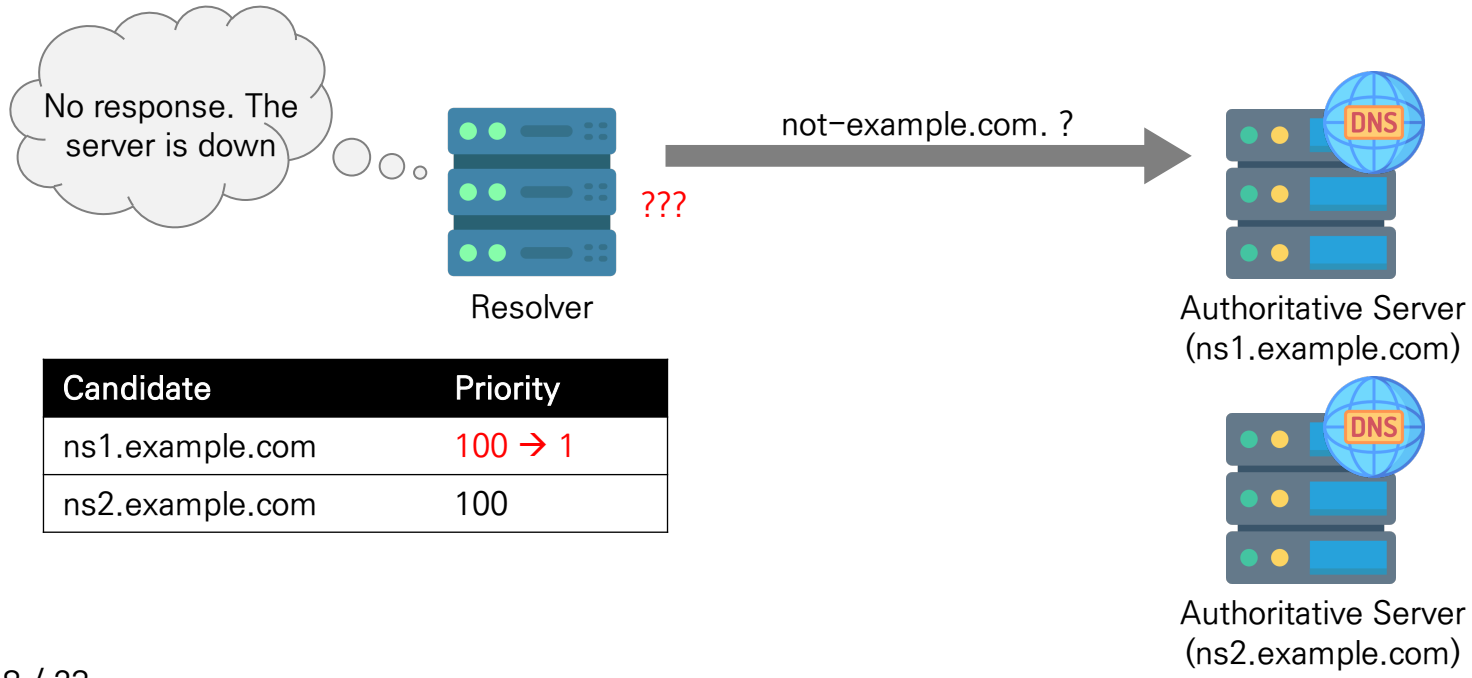


[RFC 8906] A Common Operational Problem in DNS Servers, 2020

"Failing to respond at all is always incorrect, regardless of the configuration of the server"

Flawed Recursive Resolvers Implementation

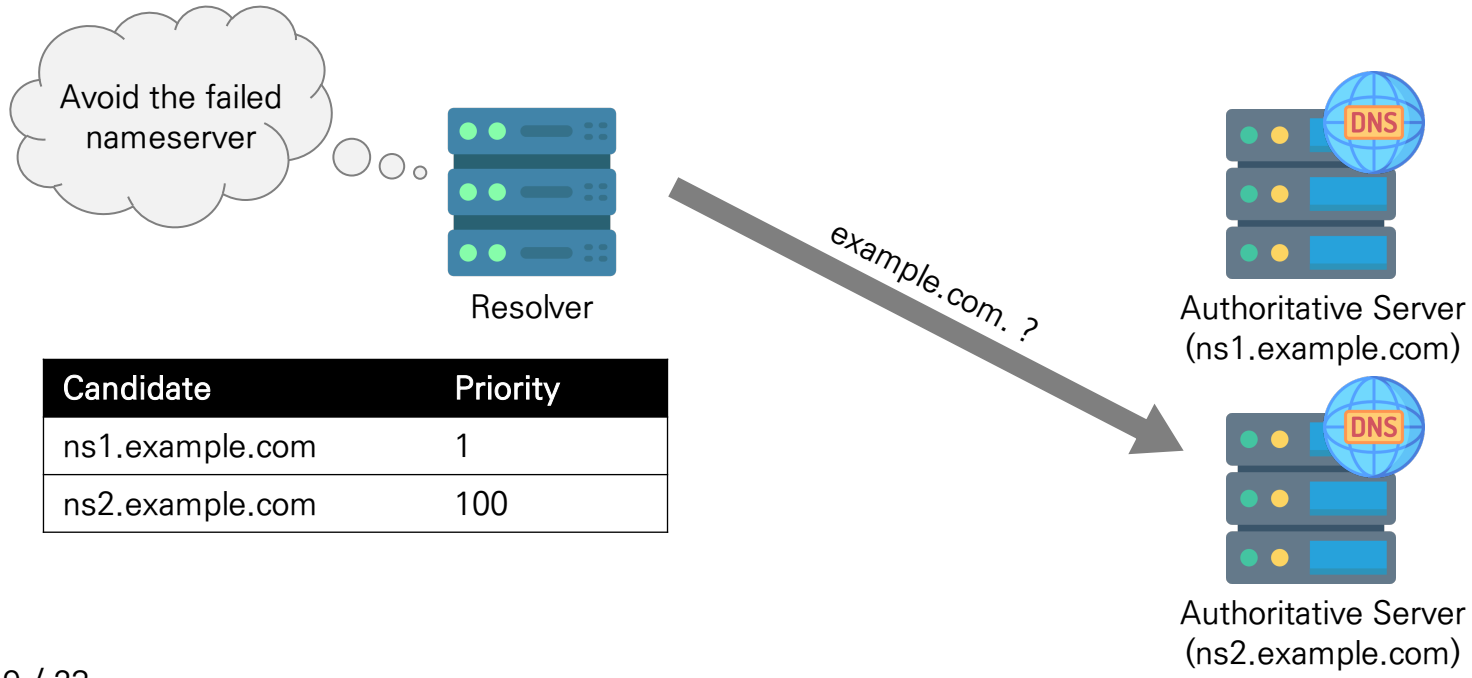
- **Recursive DNS software**
  - Prefers the nameserver with the best performance, i.e., RTT
  - Avoids the nameserver that fails to response
- **The performance metric of nameservers are globally shared by the resolvers**



Candidate	Priority
ns1.example.com	100 → 1
ns2.example.com	100

Flawed Recursive Resolvers Implementation

- **Recursive DNS software**
  - Prefers the nameserver with the best performance, i.e., RTT
  - Avoids the nameserver that fails to response
- **The performance metric of nameservers are globally shared by the resolvers**



Candidate	Priority
ns1.example.com	1
ns2.example.com	100

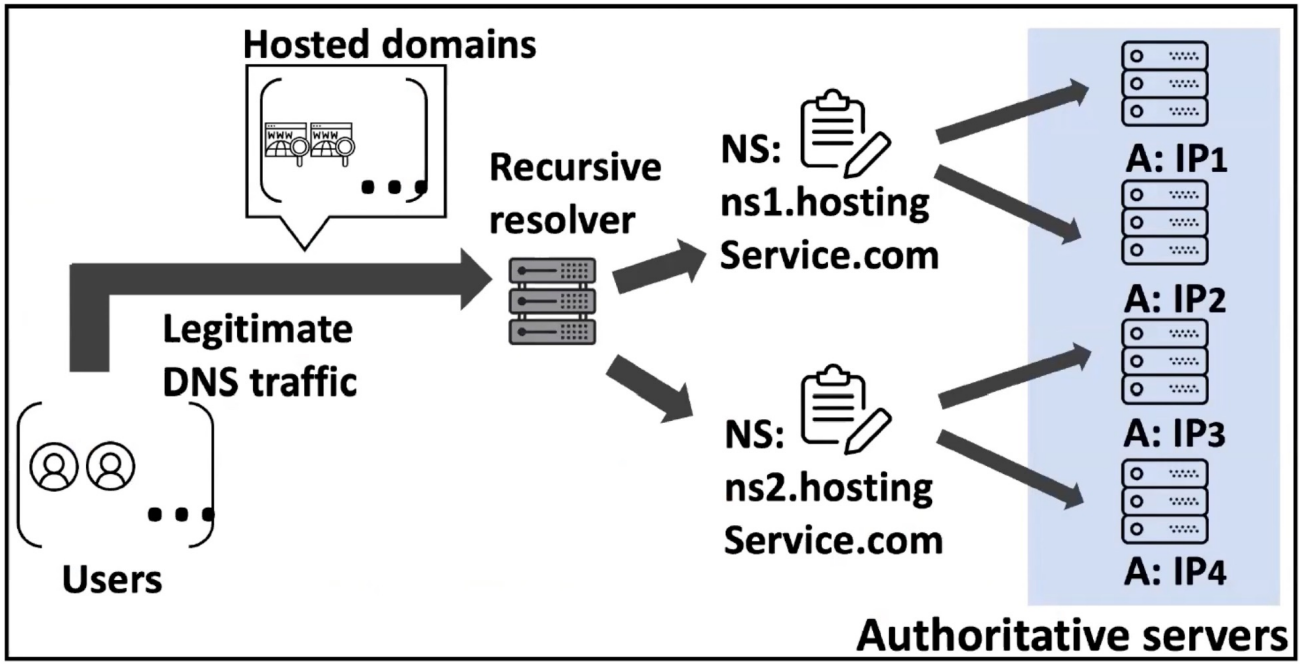
DNS Load Balancing Disabler – "Disablance"

- An adversary can manipulate the priority of authoritative servers from the view of a resolver by exploiting the response strategy
- Thus, forcing the resolver to only select a given authoritative server for future queries

- Adversaries have limited capabilities
  1. Off-path adversaries
     → Cannot hijack or eavesdrop on network traffic
  2. Only generate simple DNS queries, i.e., A records
     → Cannot craft unusual or malformed packets
  3. Expected to send packets at a low speed
     → Do not trigger the rate limit of the DNS servers

Disablance Attack Overview

- Victim's configuration

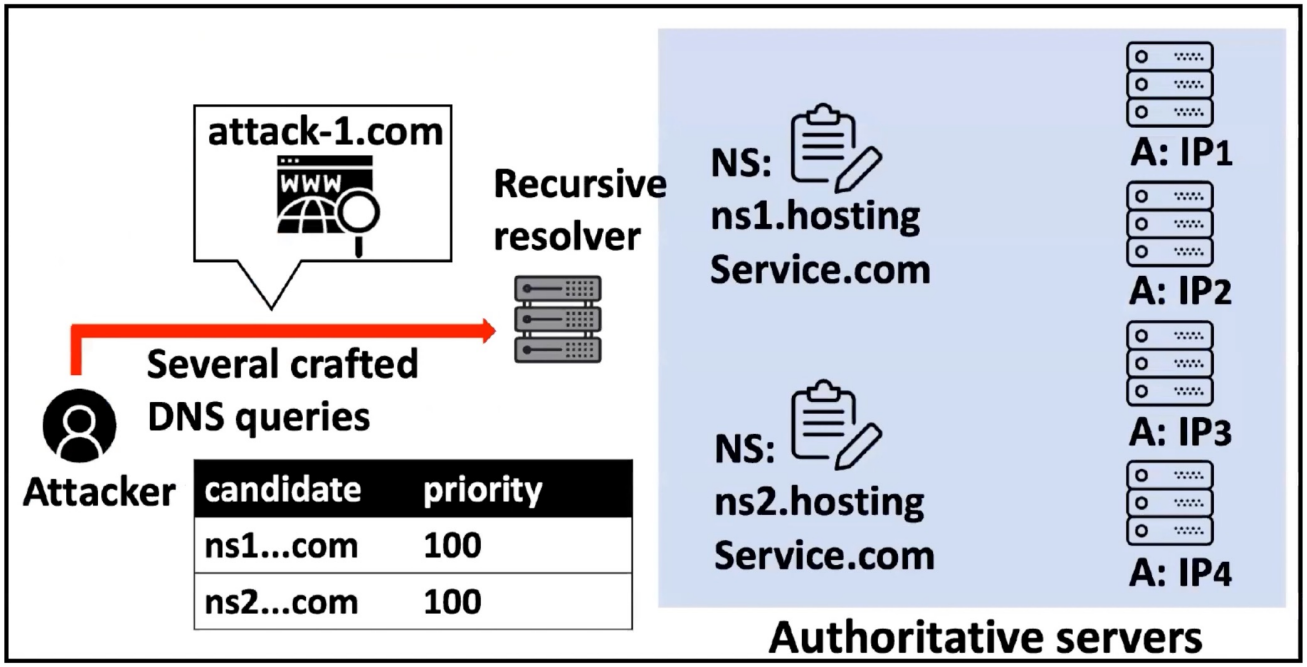



```
$ dig hostedDomain.com NS
         ...
;; ANSWER SECTION:
hostedDomain.com. 3600   IN NS ns1.hostingService.com.
hostedDomain.com. 3600   IN NS ns2.hostingService.com.

;; ADDITIONAL SECTION
ns1.hostingService.com.        3600   IN A   IP1
ns1.hostingService.com.        3600   IN A   IP2
ns2.hostingService.com.        3600   IN A   IP3
ns2.hostingService.com.        3600   IN A   IP4
```

Disablance Attack Overview

- Variant #1: Diverting legitimate traffic to a single NS

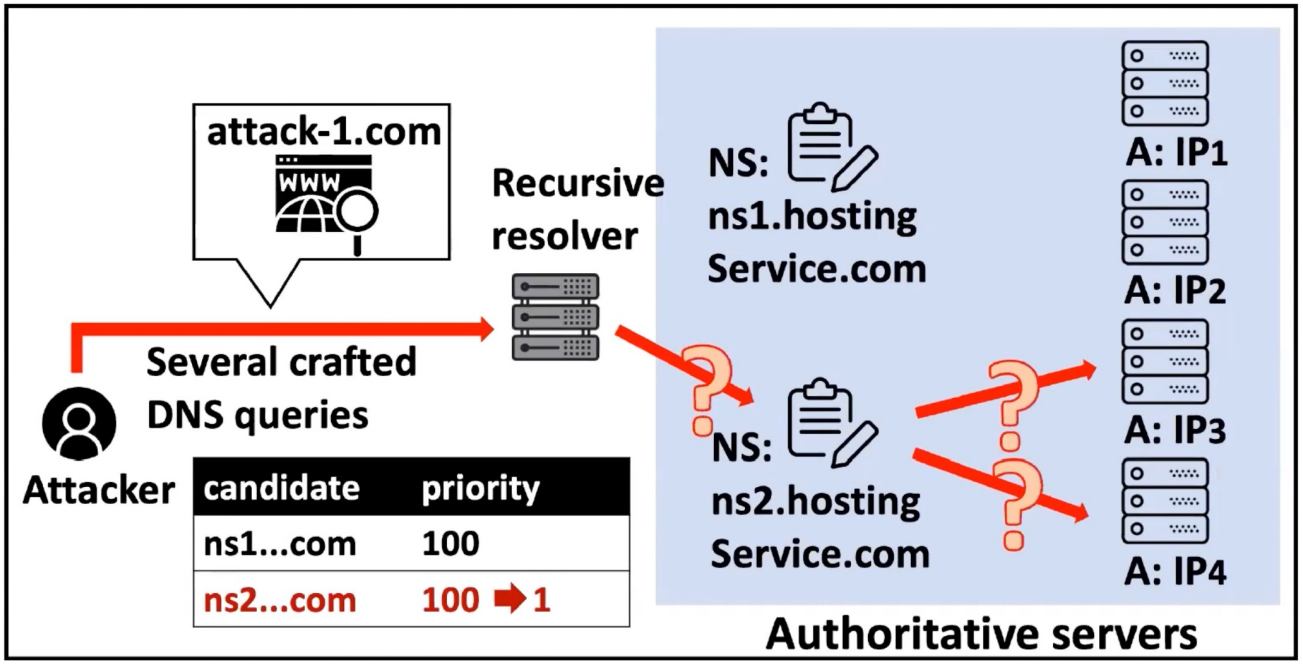



```
$ dig attack-1.com NS
          ...
;; ANSWER SECTION:
attack-1.com.   3600   IN NS ns2.hostingService.com.

;; ADDITIONAL SECTION
ns2.hostingService.com.        3600   IN A   IP3
ns2.hostingService.com.        3600   IN A   IP4
```

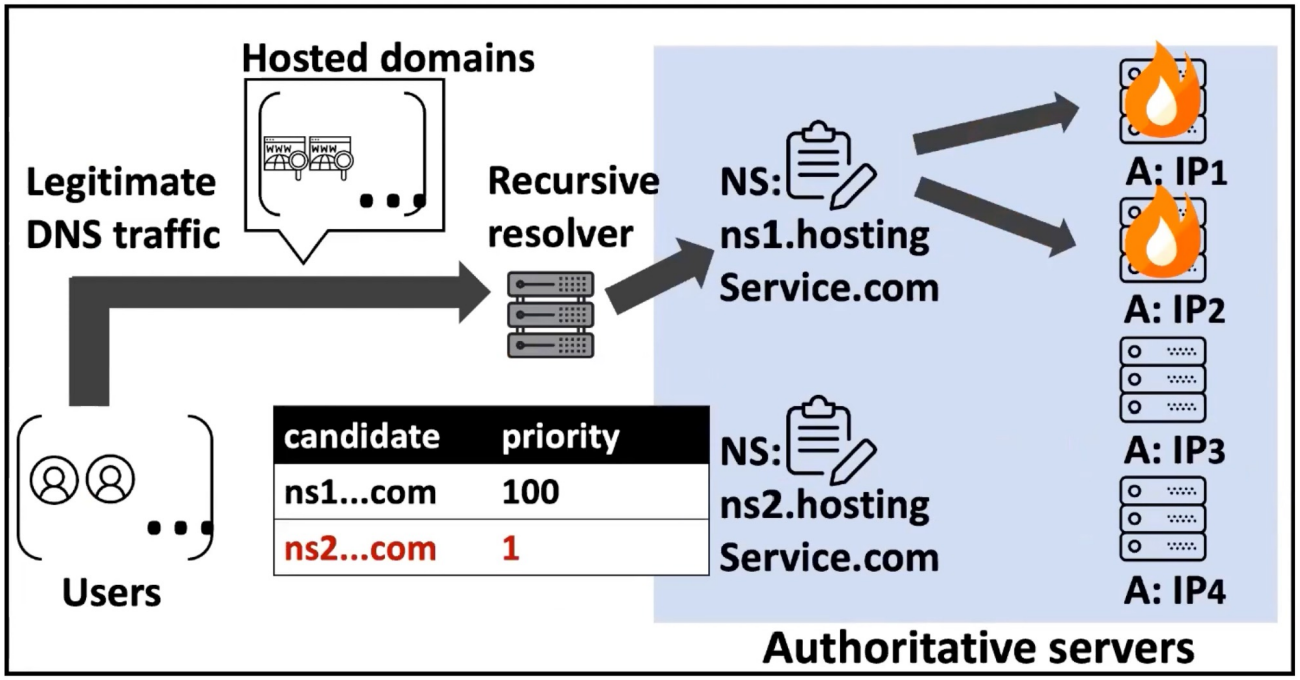
Disablance Attack Overview

- Variant #1: Diverting legitimate traffic to a single NS



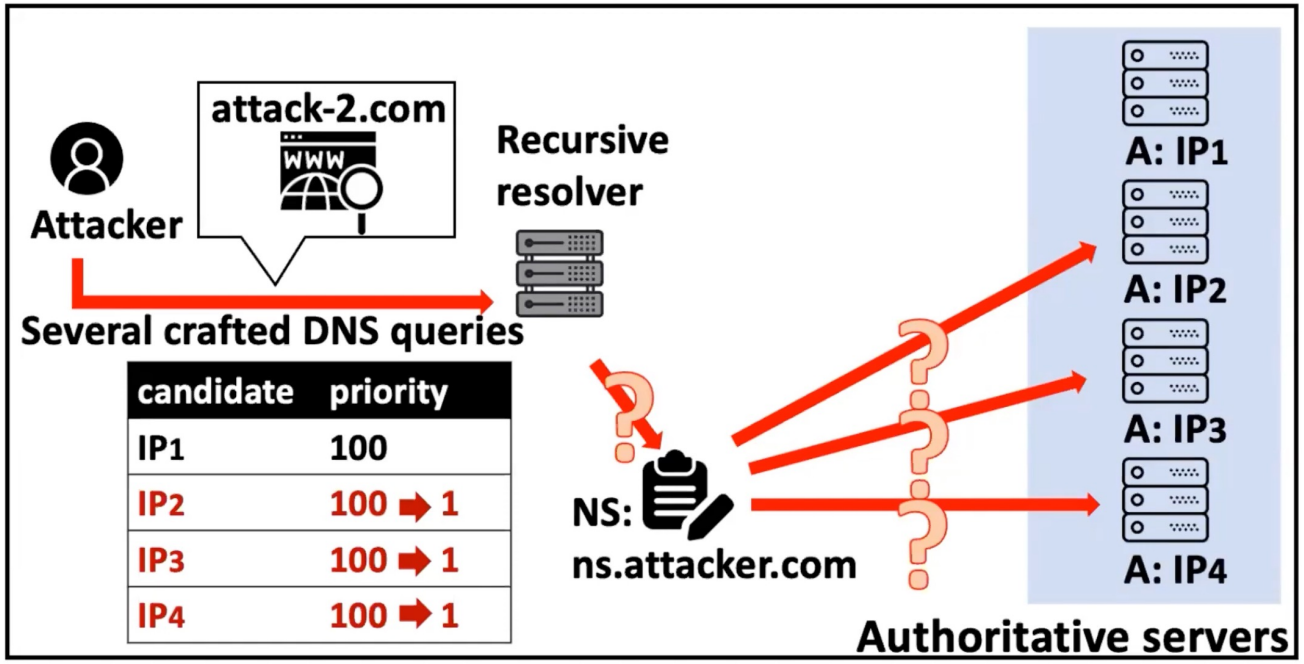
Disablance Attack Overview

- Variant #1: Diverting legitimate traffic to a single NS



Disablance Attack Overview

- Variant #2: Diverting legitimate traffic to a single IP address

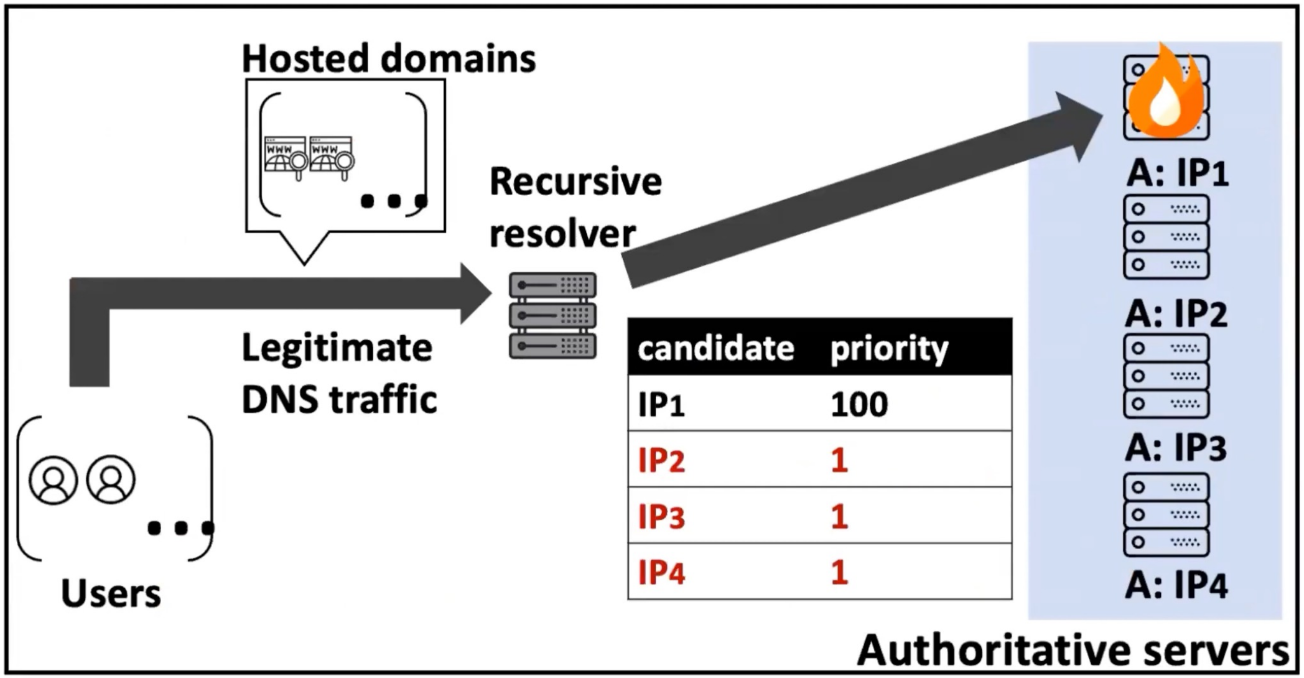



```
$ dig attack-2.com NS
          ...
;; ANSWER SECTION:
attack-2.com.   3600   IN NS ns.attacker.com.

;; ADDITIONAL SECTION
ns.attacker.com.              3600   IN A   IP2
ns.attacker.com.              3600   IN A   IP3
ns.attacker.com.              3600   IN A   IP4
```

Disablance Attack Overview

- Variant #2: Diverting legitimate traffic to a single IP address



Analysis and Evaluation – Methodology

- **Authoritative Nameserver**
  "Finding domains with misconfigured Authoritative NSs"
  - Top 1M SecRank FQDNs, Top 1M Tranco SLDs
  - Exploitable targets
    - ✓ Provides responses for its hosted domain
    - ✓ Ignores queries for a domain that is not hosted → "Silence is Golden"

Results

- **22.24% of the top 1M FQDNs and 3.94% of the top 1M SLDs are vulnerable**
  - Top 100 FQDNs consists of mobile application (SNS, mobile OS) APIs, e-commerce which are likely cloud hosted domains

Top	10	100	1K	10K	100K	1M
# FQDN	20%	29%	34.7%	26.9%	25.3%	22.2%
# SLD	10%	11%	6.8%	5.5%	4.6%	3.9%

- **Looking at individual nameservers,**
  - Top 1M FQDNs → 47,925 nameservers: 11.73% were vulnerable
  - Top 1M SLDs → 317,222 nameservers: 4.40% were vulnerable
  - Tencent Cloud hosted 6.26% of the top 1M FQDNs and 0.81% of the top 1 M SLDs

Analysis and Evaluation – Methodology

- **Authoritative Nameserver**
  "Finding domains with misconfigured Authoritative NSs"
  - Top 1M SecRank FQDNs, Top 1M Tranco SLDs
  - Exploitable targets
    - ✓ Provides responses for its hosted domain
    - ✓ Ignores queries for a domain that is not hosted → "Silence is Golden"

- **Resolvers**
  "Analyzing DNS resolver softwares"
  - DNS resolver software: BIND9 (60.2% market share in 2015), Unbound, PowerDNS, Microsoft DNS, Knot Resolver

  "Analyzing open resolvers & public DNS resolvers"
  - Google, CloudFlare, Quad9, Baidu, …

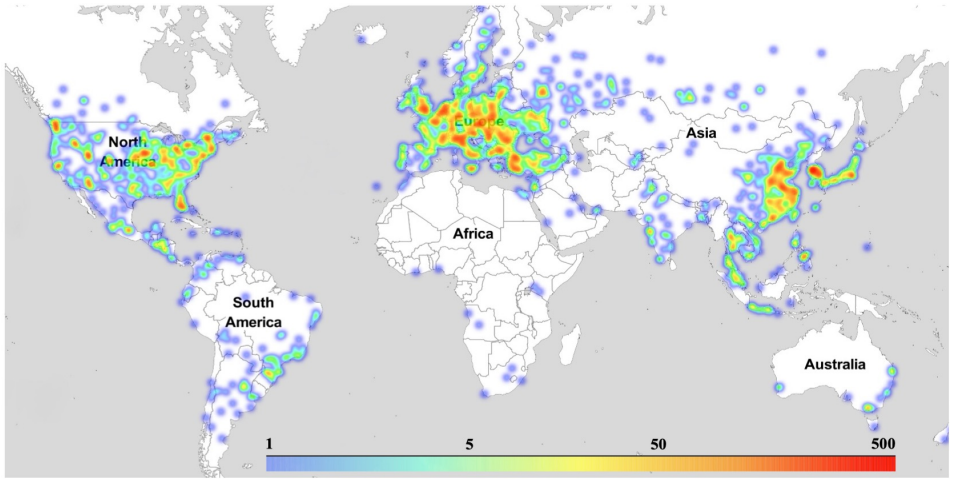
Results

- 3 out of 5 analyzed software are vulnerable
- NS selection with the lowest statistical latency when resolving a domain: BIND9 (NS record and IP address), PowerDNS (NS record)
- Unlike BIND9 and PowerDNS, Knot Resolver tries other candidates with a certain probability and restores its priority immediately when it responds successfully (known as ϵ–Greedy algorithm)

Software	Sensitive Variant	Market Share [46]
BIND9	DisablanceNS/Address	60.2+%
Unbound	-	4.8+%
PowerDNS Recursor	DisablanceNS	3.2+%
Microsoft DNS	DisablanceNS/Address	2.5+%
Knot Resolver	-	(no mention)

Results

- **Out of 37,843 stable open resolvers 14,372 (37.88%) of the tested open resolvers were vulnerable**
  - Distributed in 130 countries, 2,821 cities, and 1,778 ASes
- **10 out of 14 public resolvers were found vulnerable**
  - 45 out of 100 IP address operated by public DNS service providers
  - Vendors include Cloudflare, OneDNS, and Quad9



Vendor	Affected	# A / # T[d]
Google DNS [32]	NO	0/4
CloudFlare [22]	YES	4/14
OpenDNS [20]	NO	0/12
OneDNS [83]	YES	4/6
Quad9 [75]	YES	11/14
DNS.WATCH [27]	NO	0/4
FreeDNS [29]	YES	5/5
TWNIC Quad 101 [84]	YES	4/4
CleanBrowsing [21]	YES	6/12
Baidu DNS [15]	YES	1/1
UncensoredDNS [85]	YES	1/4
AliDNS [5]	NO	0/4
Alternate DNS [8]	YES	2/4
OpenNIC [69]	YES	7/12
Total		45/100

Mitigation

- **Authoritative NS should take responsibility since their strategy violates the DNS specification**
- **Recommendation**
  - w/ EDNS: Return REFUSED with an EDNS error code
  - w/o EDNS: Return REFUSED instead of other misleading error
  - Answering REFUSED does not introduce other DDoS attack vectors

- **Patching recursive resolver implementation is more efficient for fixing the issue**
- **Recommendation (e.g., Knot Resolver)**
  - Try other NS candidates with a predetermined probability
  - Restore the status once the nameserver responds successfully

Summary

- Authoritative server aims to protect against DNS amplification attacks, by dropping DNS queries for non-authoritative domains

- Recursive resolver aims to improve efficiency, by decreasing the priority of a nameserver when the query is timed-out

➔ Both are not compliant to the DNS standards

- Feedback from the industry
  - Tencent Cloud, Amazon, and TSSNS have taken action to fix this issue
  - DNS resolver vendors of vulnerable software acknowledged the findings, but insisted that authoritative servers should fix the issue

감사합니다

Thank you~!