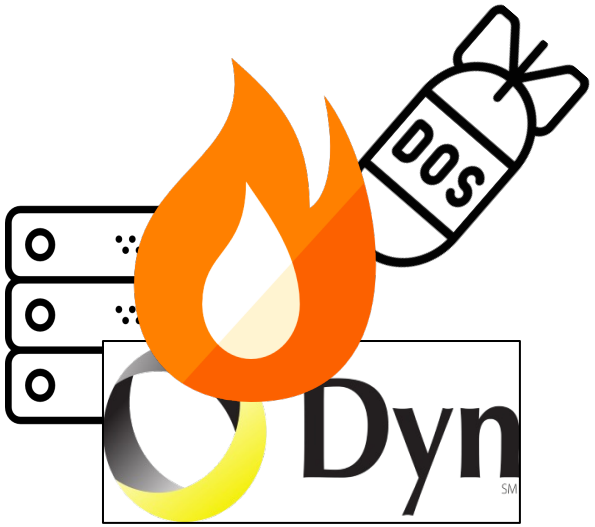
Secure Nameserver Selection Algorithm for DNS Resolvers

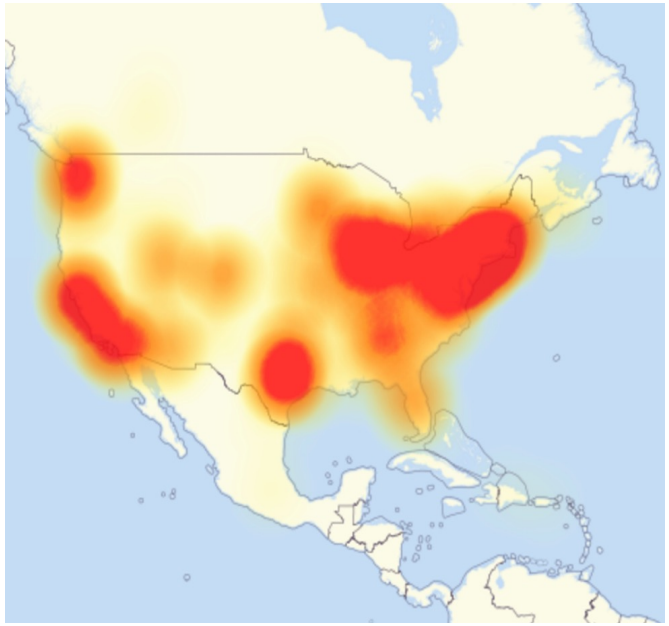
Fenglu Zhang
Tsinghua University

ICANN | NEXTGEN

The security of DNS is critical to Internet operation

- Domain Name System (DNS) is a **cornerstone** of Internet infrastructure.
- The outage of DNS can cause **severe** influence.





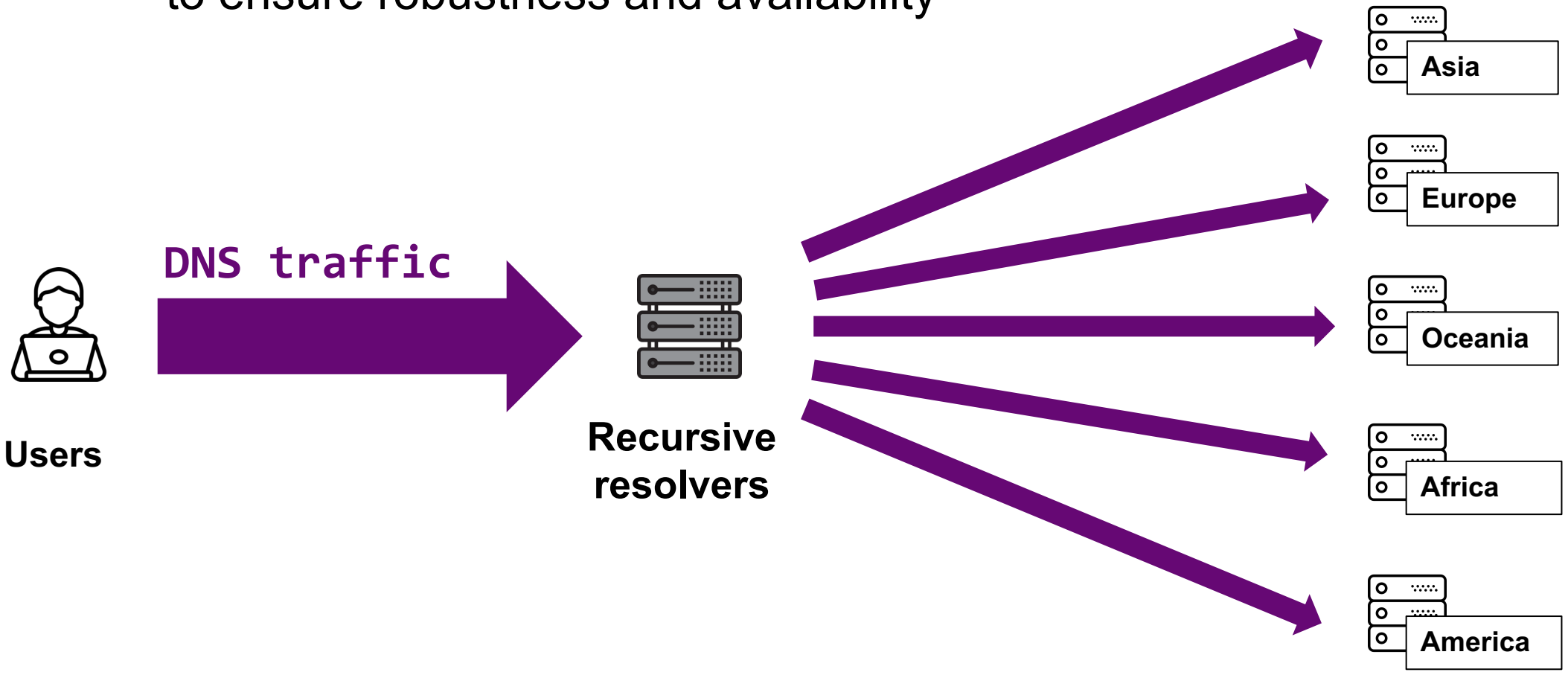
BBC CNN GitHub PayPal amazon.com

Several popular domains were unavailable in most regions
in the US during the DDoS attack on Dyn in Oct 2016

Load balancing from the view of nameservers

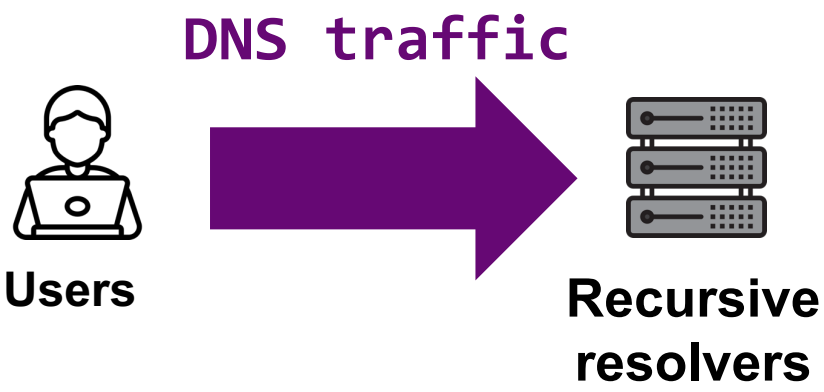
Nameservers support **load balancing mechanisms**

to ensure robustness and availability



Load balancing from the view of resolvers

- Resolvers witness multiple candidates **with limited information**
- Resolvers rely on **nameserver selection algorithm** to pick the best candidate



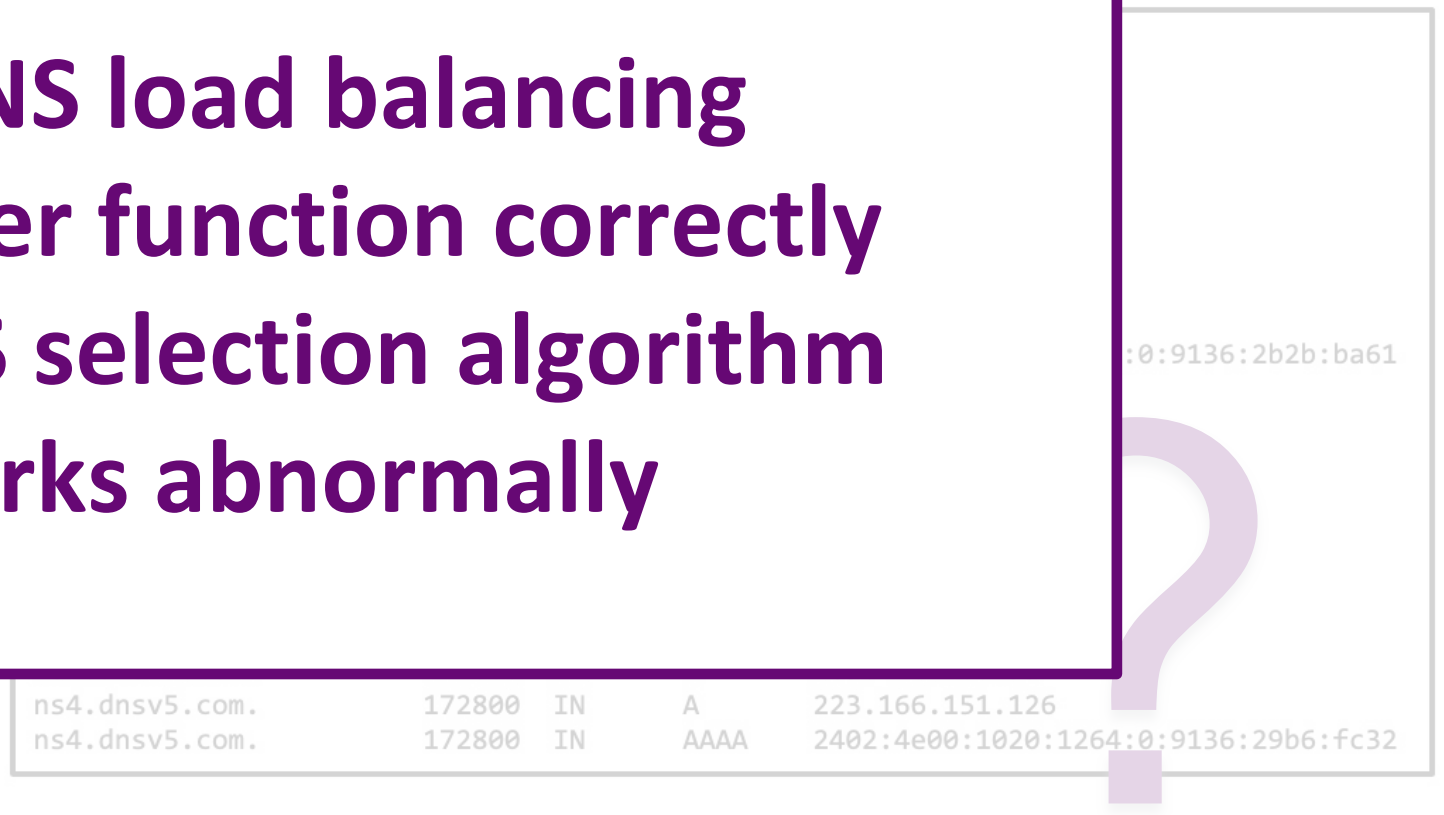

```
;; AUTHORITY SECTION:
bilibili.com.           172800  IN      NS      ns3.dnsv5.com.
bilibili.com.           172800  IN      NS      ns4.dnsv5.com.

;; ADDITIONAL SECTION:
ns3.dnsv5.com.          172800  IN      A       1.12.0.17
ns3.dnsv5.com.          172800  IN      A       1.12.0.18
ns3.dnsv5.com.          172800  IN      A       1.12.0.20
ns3.dnsv5.com.          172800  IN      A       223.166.151.16
ns3.dnsv5.com.          172800  IN      AAAA    2402:4e00:1430:1102:0:9136:2b2b:ba61
ns3.dnsv5.com.          172800  IN      A       36.155.149.211
ns3.dnsv5.com.          172800  IN      A       49.234.175.103
ns3.dnsv5.com.          172800  IN      A       61.151.180.51
ns4.dnsv5.com.          172800  IN      A       1.12.0.16
ns4.dnsv5.com.          172800  IN      A       1.12.0.19
ns4.dnsv5.com.          172800  IN      A       106.55.82.76
ns4.dnsv5.com.          172800  IN      A       117.89.178.200
ns4.dnsv5.com.          172800  IN      A       183.192.164.119
ns4.dnsv5.com.          172800  IN      A       183.47.126.155
ns4.dnsv5.com.          172800  IN      A       223.166.151.126
ns4.dnsv5.com.          172800  IN      AAAA    2402:4e00:1020:1264:0:9136:29b6:fc32
```

Load balancing from the view of resolvers

- Resolvers witness multiple candidates **with limited information**
- Resolve candidate

The NS load balancing will never function correctly if the NS selection algorithm works abnormally

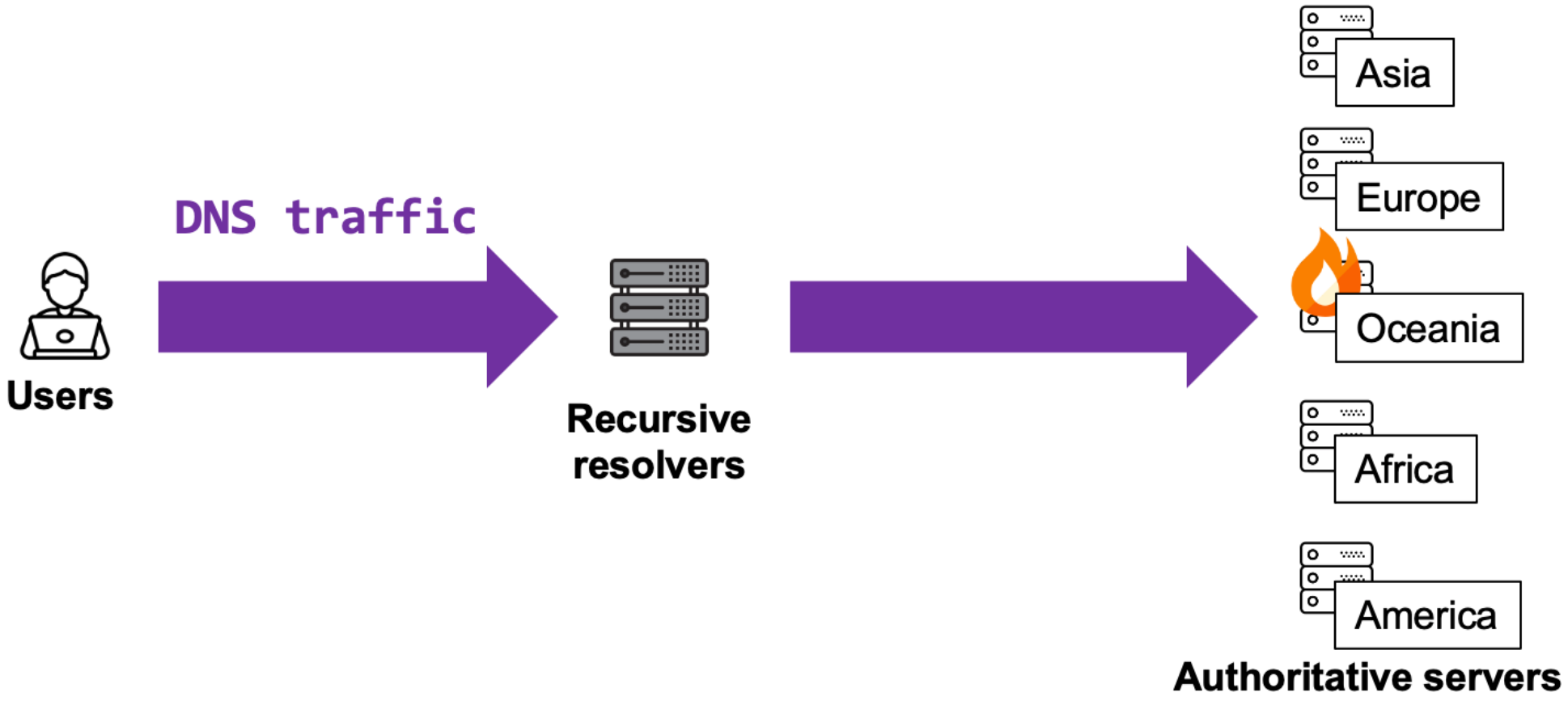
Users



Security risks of vulnerable NS selection

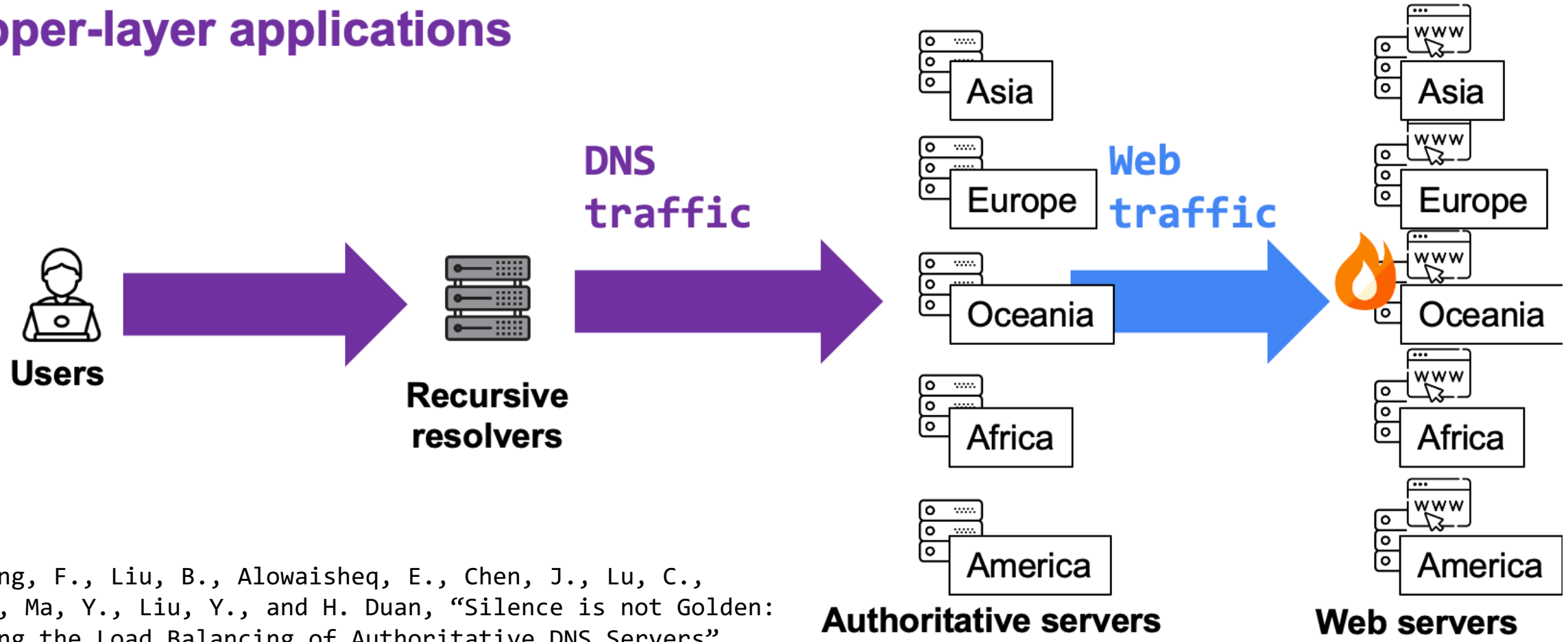
Security risks of vulnerable NS selection

Impact 1: overloading authoritative DNS servers with legitimate traffic



Security risks of vulnerable NS selection

Impact 2: disrupting DNS-based load balancing of upper-layer applications



Ref: Zhang, F., Liu, B., Alowaisheq, E., Chen, J., Lu, C., Song, L., Ma, Y., Liu, Y., and H. Duan, "Silence is not Golden: Disrupting the Load Balancing of Authoritative DNS Servers", DOI 10.1145/3576915.3616647, 2023, ACM CCS

Summary

- **The risks are critical VS. The standardization of NS selection lack**
  - [RFC1034] vaguely suggests that resolvers should *“find the best server to ask.”*
- To fill the gap, we summarize the published paper and propose this research to
  - **Reveal the mainstream nameserver selection algorithm**
  - **Summarize the uncovered vulnerabilities abused NS selection**
  - **Provide recommendations to defend against the security risks**

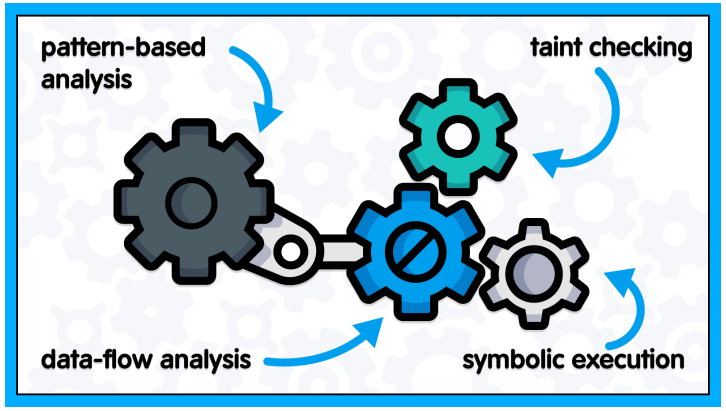
Mainstream NS selection algorithms

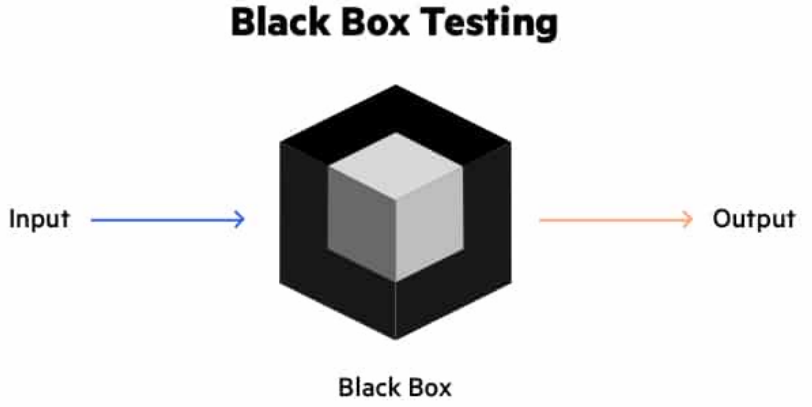
Methodology

- **Refer to four published research papers**
  1. Zhang, F., Liu, B., Alowaisheq, E., Chen, J., Lu, C., Song, L., Ma, Y., Liu, Y., and H. Duan, “Silence is not Golden: Disrupting the Load Balancing of Authoritative DNS Servers”, DOI 10.1145/3576915.3616647, 2023, ACM CCS
  2. Zhang, F., Lu, C., Liu, B., Duan, H., and Y. Liu, "Measuring the Practical Effect of DNS Root Server Instances: A China-Wide Case Study", 2022, PAM
  3. Yu, Y., Wessels, D., Larson, M., and L. Zhang, "Authority server selection in DNS caching resolvers", 2012,
  4. Müller, M., Moura, G.C.M., Schmidt, R. de O., and J.Heidemann, "Recursives in the Wild: Engineering Authoritative DNS Servers", DOI 10.1145/3131365.3131366, 2017

Methodology

- **Methodologies of selected papers**
  - White-box view
    - Most of DNS software is open-source
    - Option
      - Static analysis
      - Dynamic debugging
  - Black-box view
    - Some DNS software, open resolvers, and public recursive services are not open-source
    - Option
      - Simulation in lab environments
      - Sending testing packets



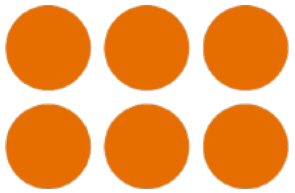


Pic source: https://pvs-studio.com/en/blog/posts/1048/
https://www.imperva.com/learn/application-security/black-box-testing/

Result: the definition of the best server

- [RFC1034] vaguely suggests that resolvers should *"find the best server to ask."*
  - **What is the definition of the best server?**

BIND9



PowerDNS

Always pick the candidate with the highest **priority**

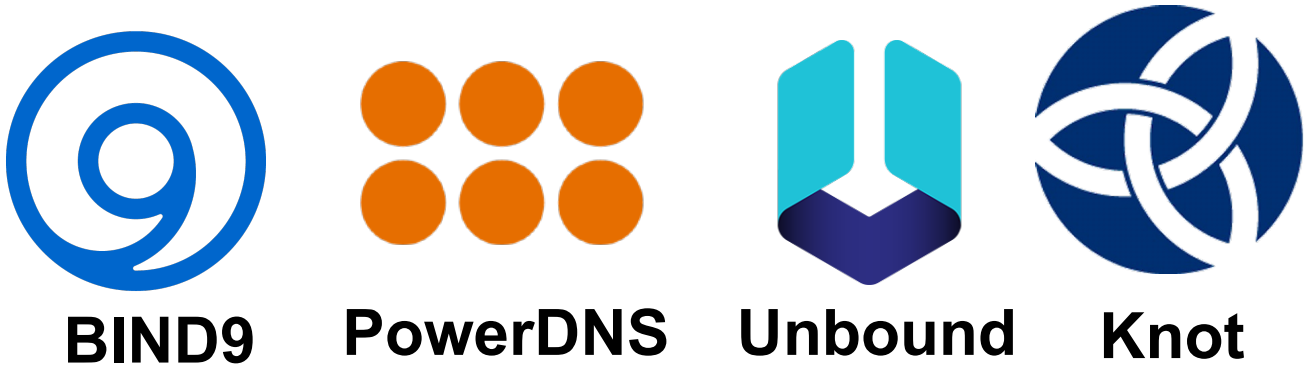
~95% chances: the highest **priority**,
~5% pick randomly

Knot

Unbound

Pick randomly in a range of **priority**

Result: the definition of the priority



1. The priority is the adjusted SRTT (Smoothed Round Trip Time)
2. Apply a penalty to the SRTT while detecting failure (e.g., DNSSEC failure)

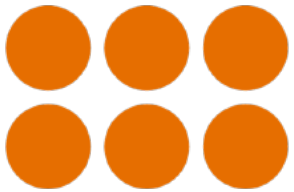
Result: store the status of the NS

BIND9

Knot

Share the status at the level of IP address

Share the status at the level of NS record



PowerDNS

Unbound

maintaining the status for each delegation **individually**

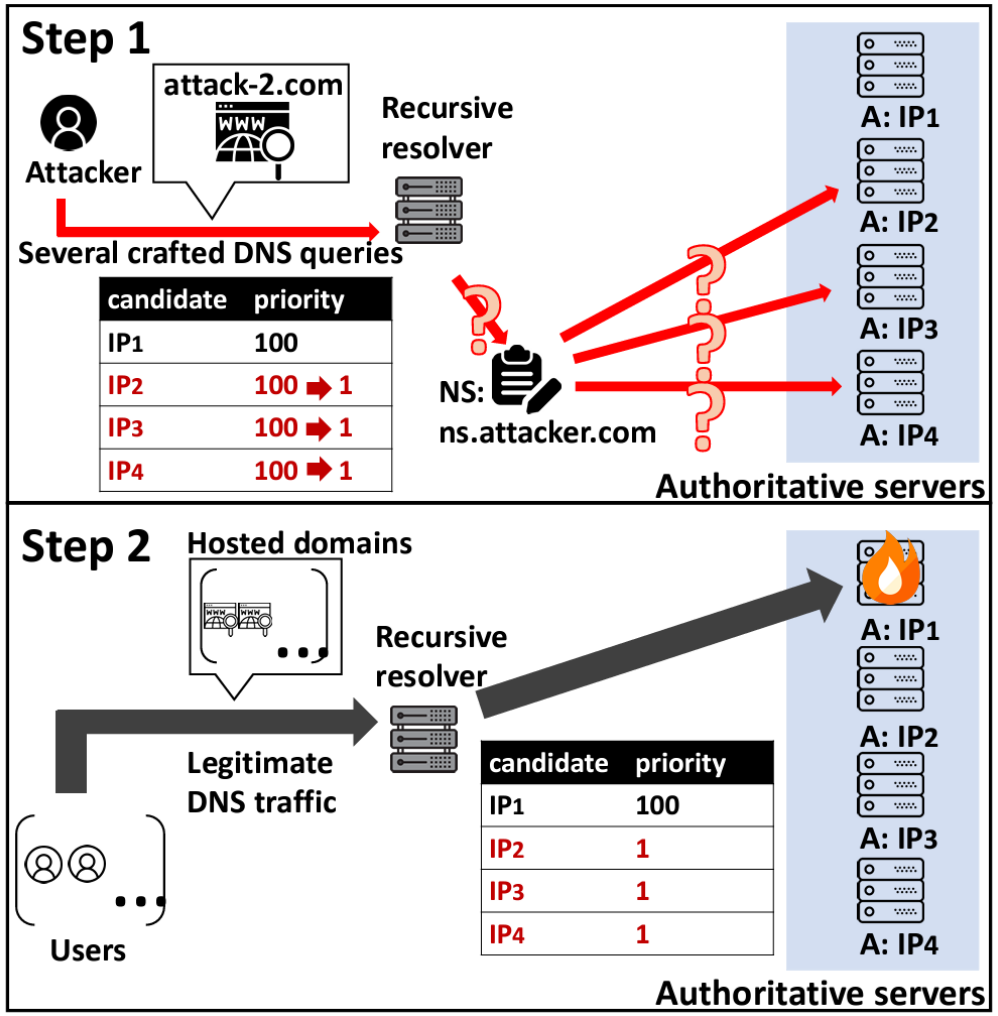
Vulnerabilities exploiting NS selection algorithm

Vulnerabilities exploiting NS selection algorithm

- **V1: Disablance Attack**
- **V2: Subverting SRTT Algorithm**
- **V3: Cyclical Queries**

Vulnerabilities exploiting NS selection algorithm

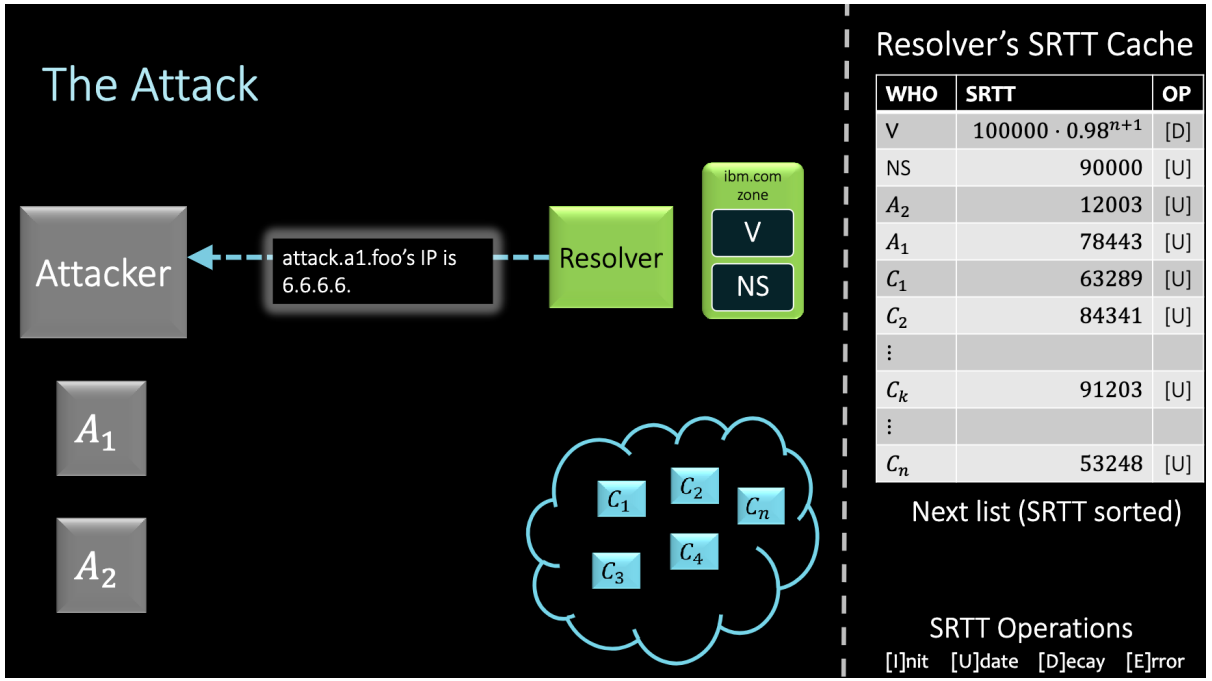
- **V1: Disablance Attack**
  - allows disrupting load balancing of NS at a low cost
  - exploits shared status of NS + penalty mechanism
- V2: Subverting SRTT Algorithm
- V3: Cyclical Queries



Zhang, F., Liu, B., Alowaisheq, E., Chen, J., Lu, C., Song, L., Ma, Y., Liu, Y., and H. Duan, "Silence is not Golden: Disrupting the Load Balancing of Authoritative DNS Servers", DOI 10.1145/3576915.3616647, 2023, ACM CCS

Vulnerabilities exploiting NS selection algorithm

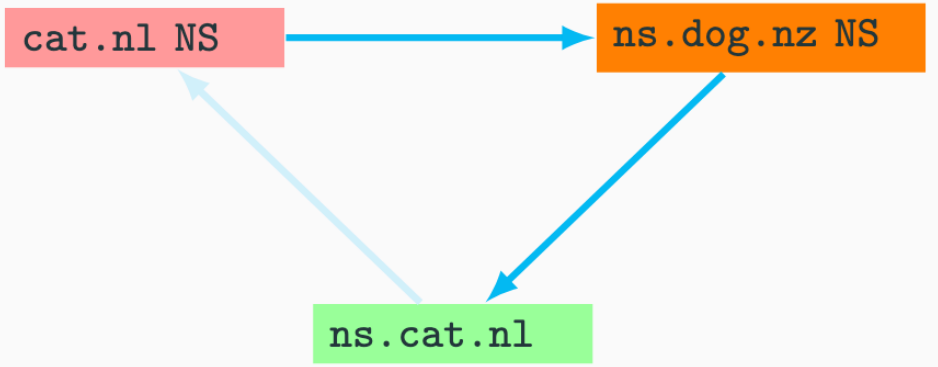
- V1: Disablance Attack
- **V2: Subverting SRTT Algorithm**
  - allows manipulating NS selections
  - exploits shared status of NS + penalty mechanism
- V3: Cyclical Queries

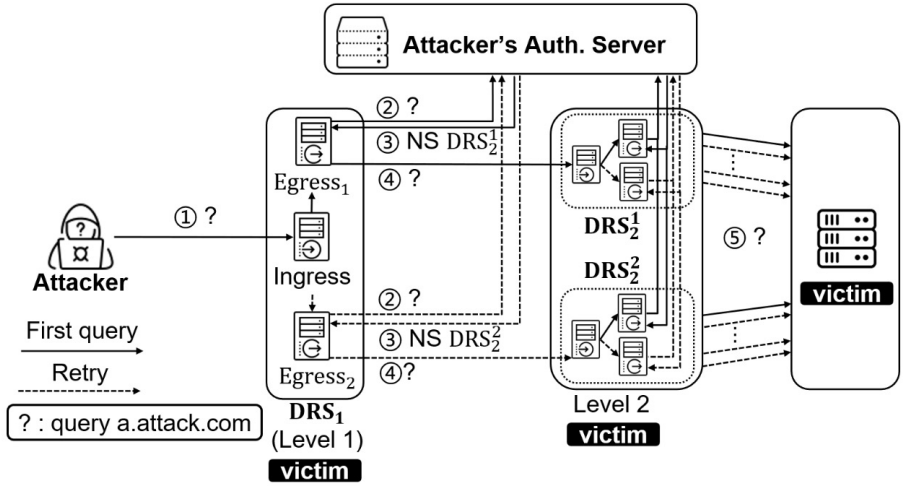


Hay, R., Kalechstein, J., and G. Nakibly, "Subverting BIND's SRTT Algorithm Derandomizing NS Selection", USENIX 7th Workshop on Offensive Technologies (WOOT 13), 2013

Vulnerabilities exploiting NS selection algorithm

- V1: Disablance Attack
- V2: Subverting SRTT Algorithm
- **V3: Cyclical Queries**
  - allows traffic amplification and DoS attack
  - exploit the unbounded designs of NS selection





- Moura, G., Castro, S., Heidemann, J., and W. Hardaker, "TsuNAME: exploiting misconfiguration and vulnerability to DDoS DNS", DOI 10.1145/3487552.3487824, 2021
- Xu, W., Li, X., Lu, C., Liu, B., Duan, H., Zhang, J., Chen, J., and T. Wan, "TsuKing: Coordinating DNS Resolvers and Queries into Potent DoS Amplifiers", DOI 10.1145/3576915.3616668, 2023

Recommendations

Our recommendations

- **R1: Balance between Optimization and Exploration**
- **R2: Independent Nameserver Status**
- **R3: Bounding Work**

Our recommendations

- **R1: Balance between Optimization and Exploration**
  - Vulnerabilities (V1-V2) abuse the selection of the candidate with the best performance and manipulate the NS selection of resolvers
  - We recommend a balance between optimization and exploration (as Knot and Unbound)
- **R2: Independent Nameserver Status**
- **R3: Bounding Work**

Our recommendations

- R1: Balance between Optimization and Exploration
- **R2: Independent Nameserver Status**
  - Vulnerabilities (V1-V2) abuse the shared status of NS and manipulate the NS selection of resolvers
  - We recommend maintaining independent status for each domain (as Unbound)
- R3: Bounding Work

Our recommendations

- R1: Balance between Optimization and Exploration
- R2: Independent Nameserver Status
- **R3: Bounding Work**
  - Cyclical queries (V3) abuse unbounded designs of resolvers and lead to the DoS attack
  - We recommend preventing cyclical queries and aborting with an error

Summary

- In this work, we
  - Reveal the mainstream nameserver selection algorithm
  - Summarize the uncovered vulnerabilities abused NS selection
  - Provide recommendations to defend against the security risks
- **We suggest**
  - **Developer of DNS software:** consider our recommendations and redesign the vulnerable algorithm
  - **Vendor of public DNS services:** consider deploying a monitor mechanism to defend against uncovered attacks

Thanks for listening
Any questions and comments are welcome

zfl20@tsinghua.org.cn

ICANN | NEXTGEN