usenix
THE ADVANCED
COMPUTING SYSTEMS
ASSOCIATION

33RD USENIX
SECURITY SYMPOSIUM

# *Cross the Zone:* Toward a Covert Domain Hijacking via Shared DNS Infrastructure

Yunyi Zhang, Mingming Zhang, Baojun Liu, Zhan Liu, Jia Zhang, Haixin Duan,
Min Zhang, Fan Shi, Chengxi Xu

Presenter: **Chaoyi Lu**
Posdoctoral researcher, Tsinghua University
https://chaoyi.lu

# Brief Summary

XDAuth

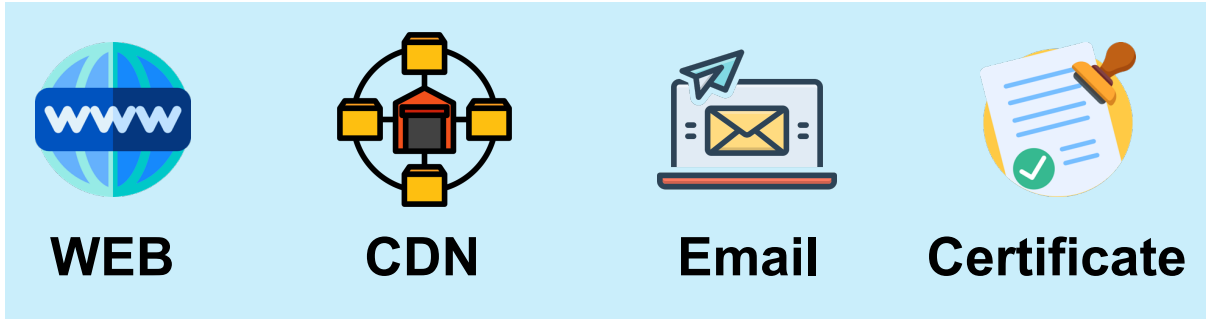
- **We uncover a prevalent covert DNS infrastructure deployment practice: shared nameservers infrastructure.**

- **The XDAuth attack exploits well-known DNS hosting platforms to take over domain names of enterprises.**

# Domain Name System

XDAuth

❖ Translating domain names to IP addresses

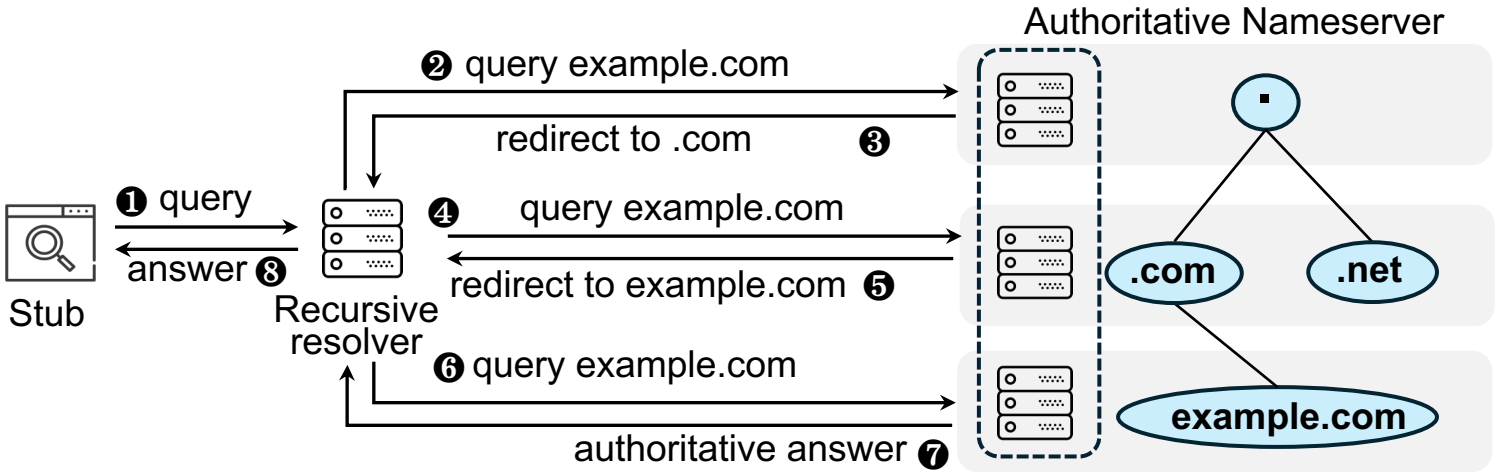



entry point of many Internet activities

# Domain Name System

XDAuth

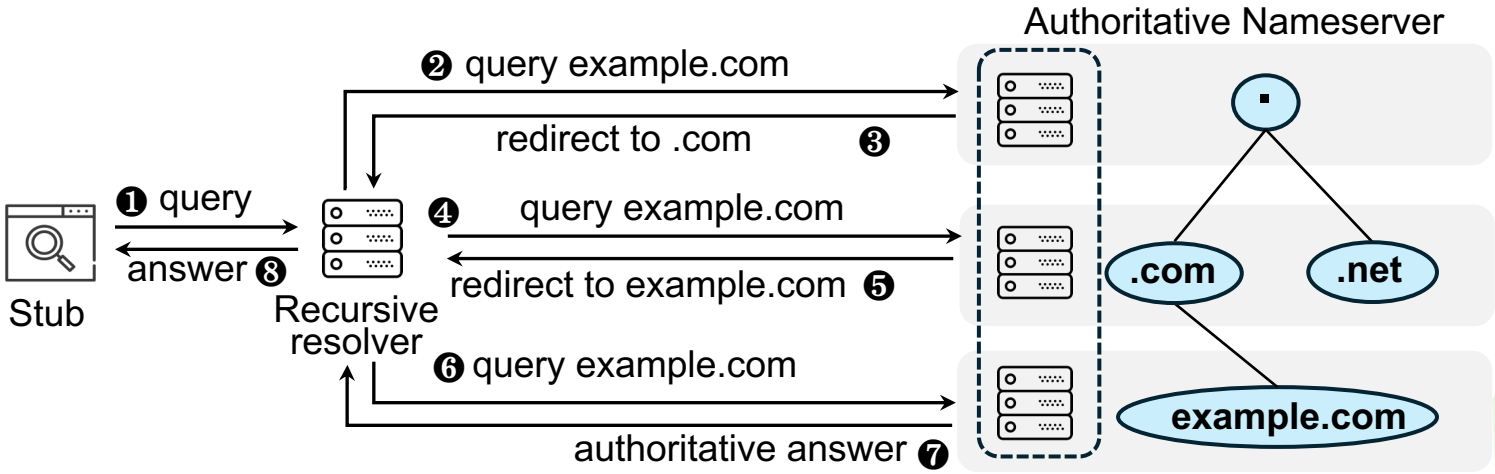
- Translating domain names to IP addresses
- Resolution process



# Domain Name System

XDAuth

- Translating domain names to IP addresses
- Resolution process




## DNS hosting platforms

Amazon Route 53

digicert DNS Made Easy

阿里云 aliyun.com

NS1. an IBM Company

DNSPOD

# Domain Hijacking (from authoritative)

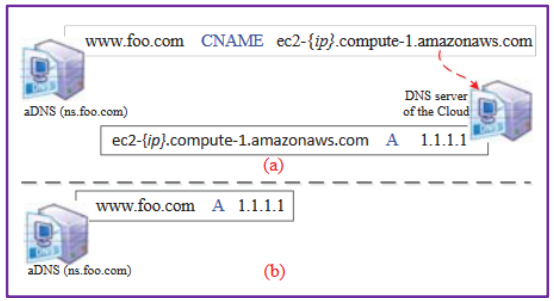
XDAuth

## ❖ Target

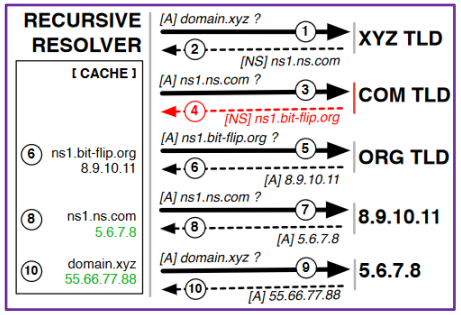
- Unauthorized manipulation of domain name resource records

## ❖ Threat Model

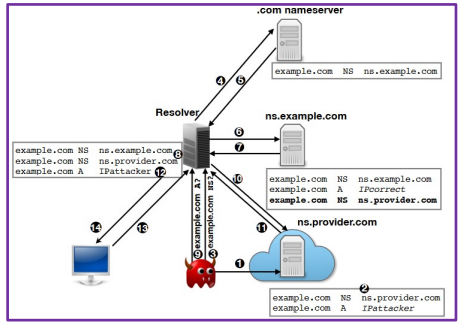
- Nameserver domain squatting
- Nameserver relocation



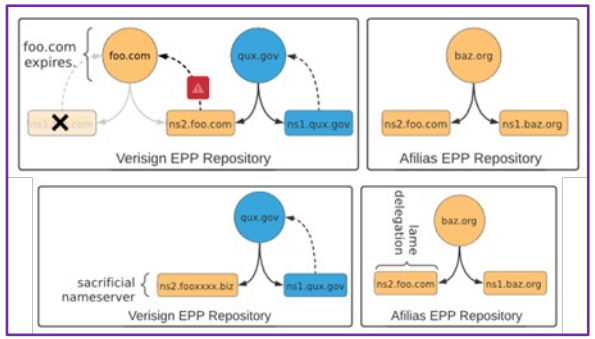

Dangling records
2016




Nameserver squatting
2017




Zaw attack
2020




Sacrificial NS
2021

# Domain Hijacking Mitigation

XDAuth

## ❖ Nameserver Configuration Restriction

- Do not allow the configuration of invalid NS records to prevent user typo

## ❖ Domain Ownership verification

- DNS hosting providers refuse unauthorized domain claim

## ❖ NS Relocation Check

- Prevent attackers from obtaining exploitable NS

## ❖ Self-controlled NS

- Prevent attackers from obtaining NS domain

**Google**
google.com NS ns4.google.com

**BBC**
bbc.com NS dns0.bbc.com.

# Question

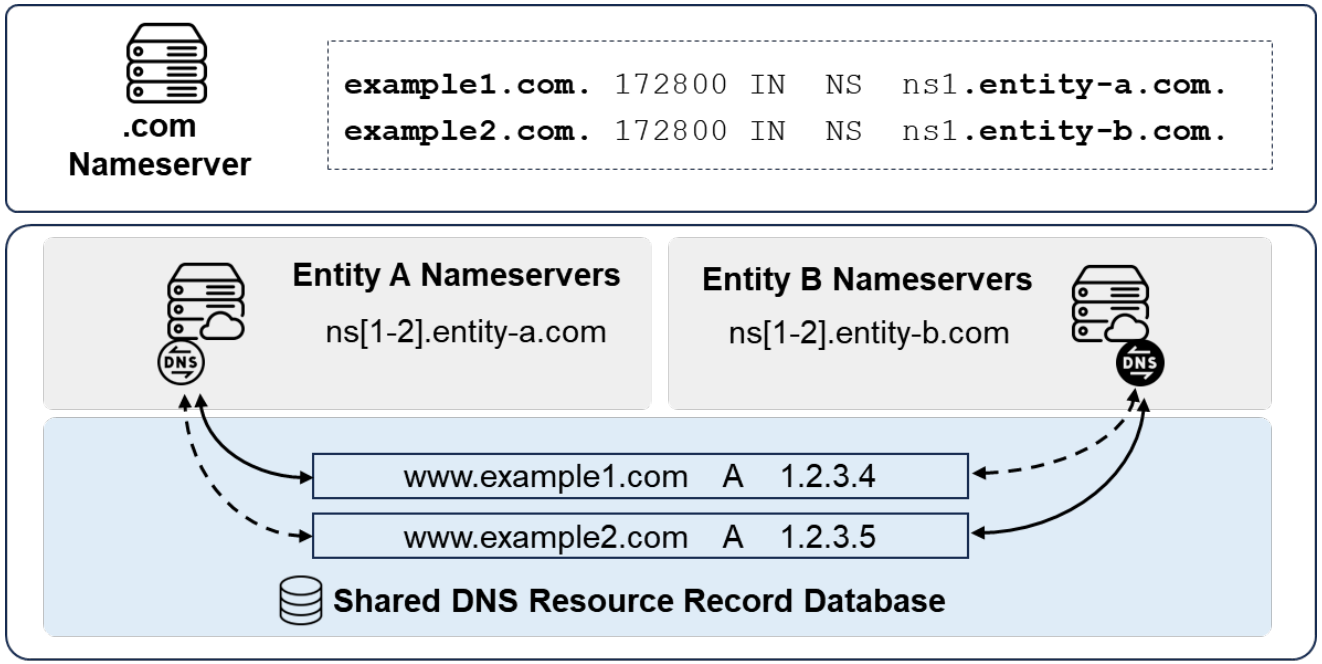
**With the protective measures mentioned above, is domain takeover still possible?**

Yes. **XDAuth** uncovers a new attack surface in the DNS infrastructure: **shared nameservers infrastructure**.

# XDAuth Attack

## ❖ Shared nameserver

- Different NS domain names rely on the same underlying infrastructure
- Entities: DNS host provider, Registrar, and other enterprises, e.g., BBC, Nike

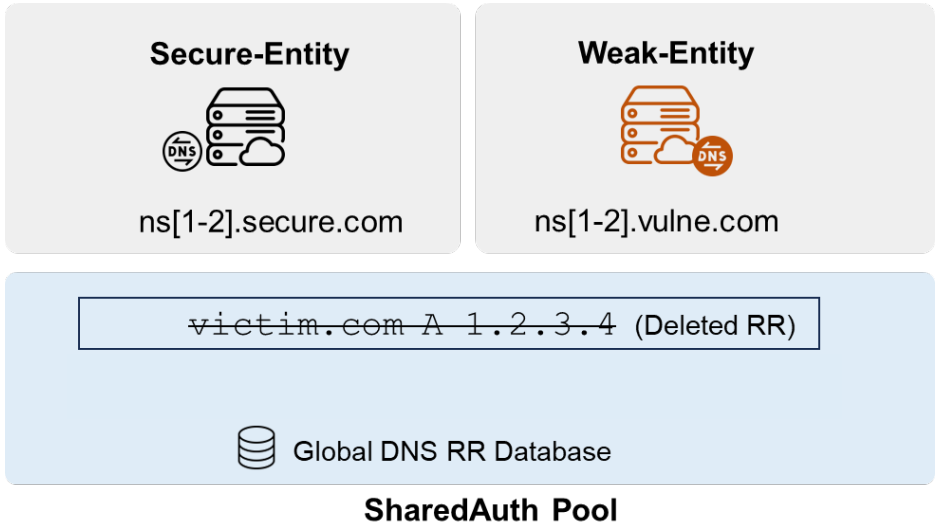


# XDAuth Attack

## ❖ Threat model

- ☐ Conditions
  - delegated to shared nameserver
  - canceled the service

false sense of safety




**victim.com NS ns1.secure.com**

# XDAuth Attack

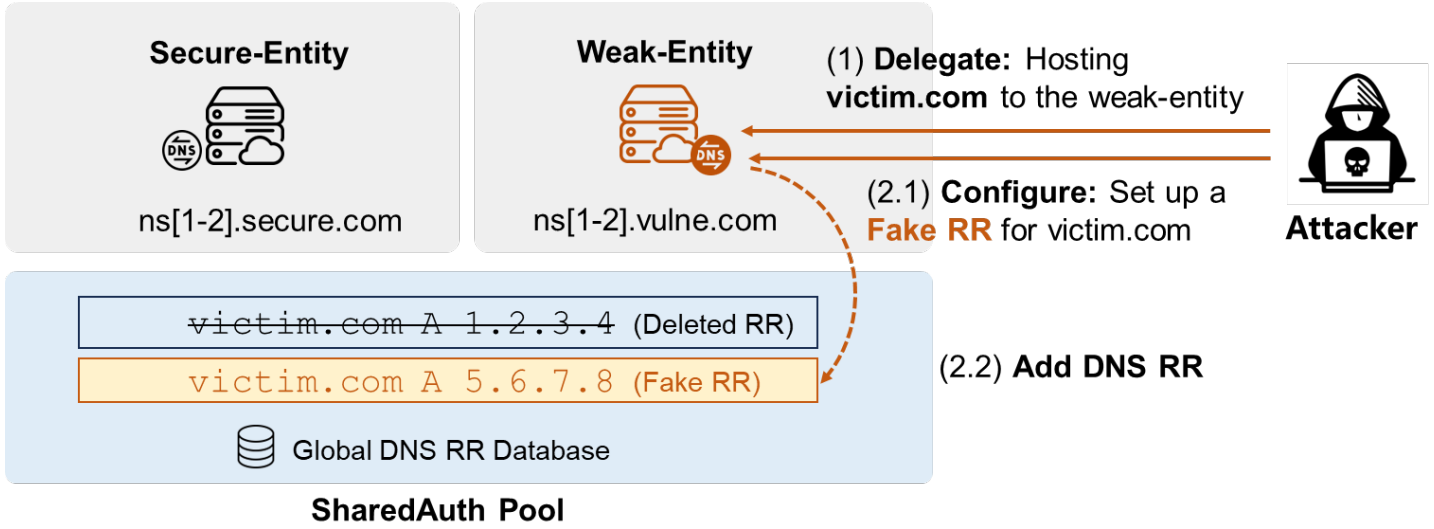
## ❖ Threat model

- Conditions
  - delegated to shared nameserver
  - canceled the service

  false sense of safety

- Target
  - break the boundary of nameserver
  - hijack domain by shared nameserver

  hijack private domain




**victim.com NS ns1.secure.com**

# XDAuth Attack

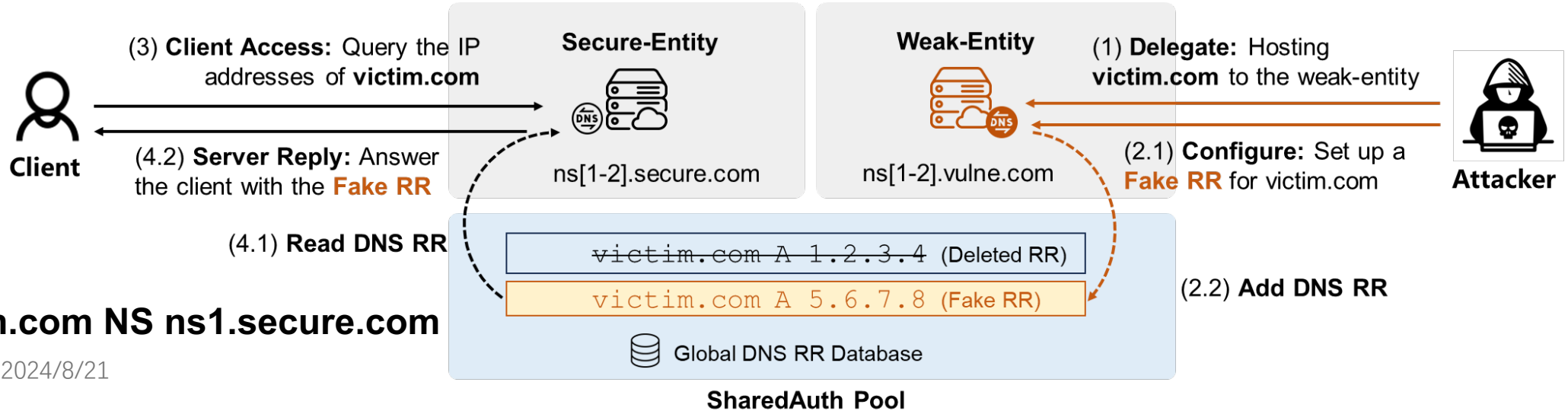
## ❖ Threat model

- Conditions
  - delegated to shared nameserver
  - canceled the service

  false sense of safety

- Target
  - break the boundary of nameserver
  - hijack domain by shared nameserver

  hijack private domain



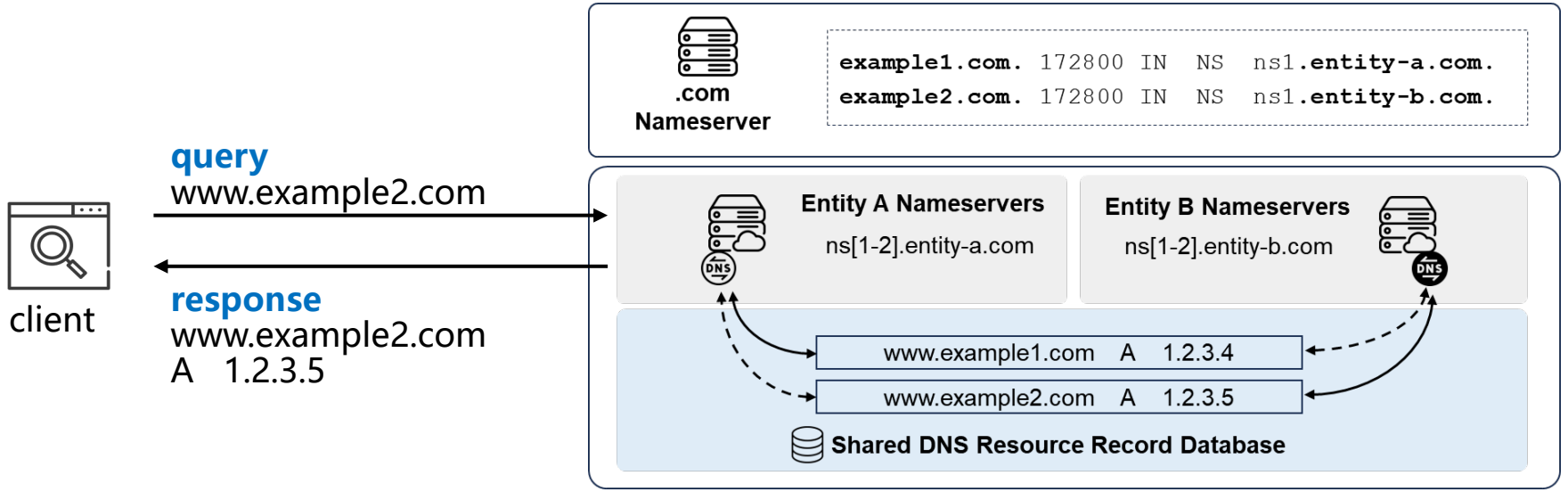

**victim.com NS ns1.secure.com**

# Question

**How to discover the shared nameservers hidden behind the services?**

## ❖ Response from shard nameservers

- nameservers respond with the correct response, outside of the delegation
- ***ns1.entity-a.com*** respond the query of domain ***www.example2.com***




**cross-resolution verification**

## ❖ Step 1: Discovering NS Candidates of Hosting Service

72

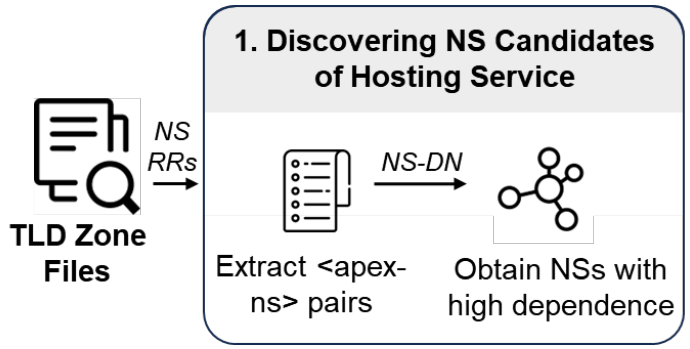
Research Report

+

10,90

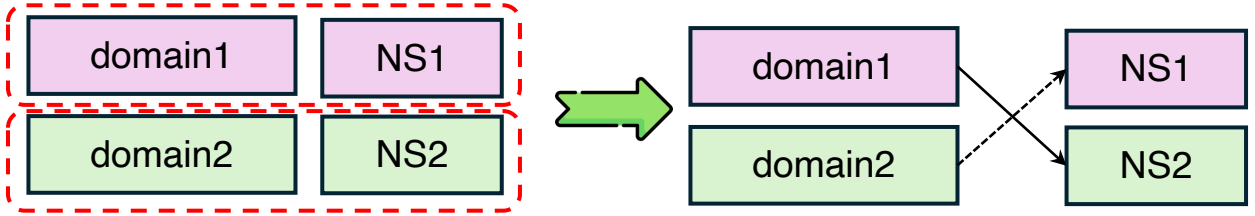
TLD zonefile

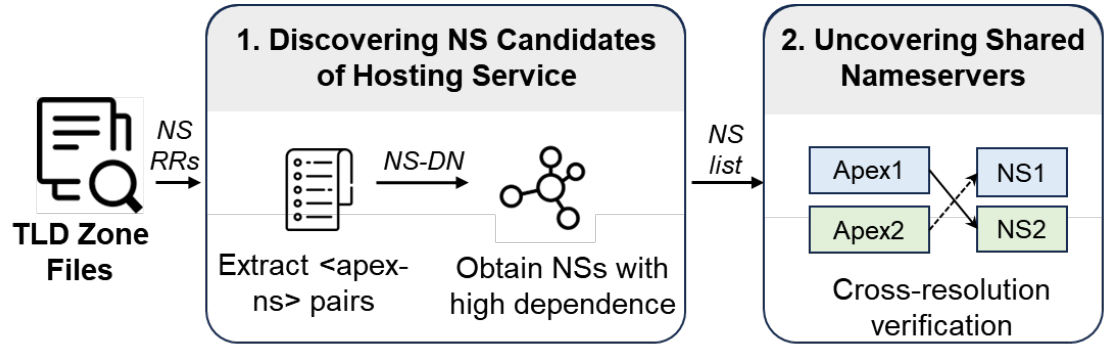
⇒ 25,310 NS seeds



## ❖ Step 2: Uncovering Shared Nameservers

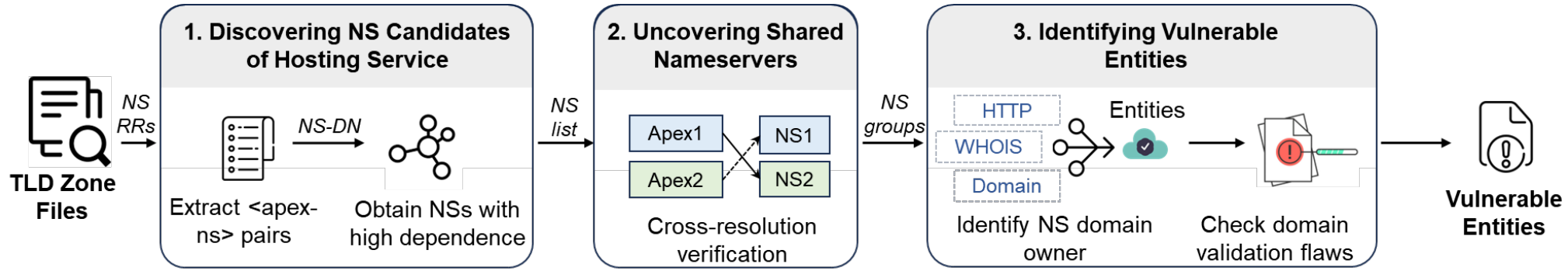
**cross-resolution verification**



## ❖ Step 3: Identifying Vulnerable Entities

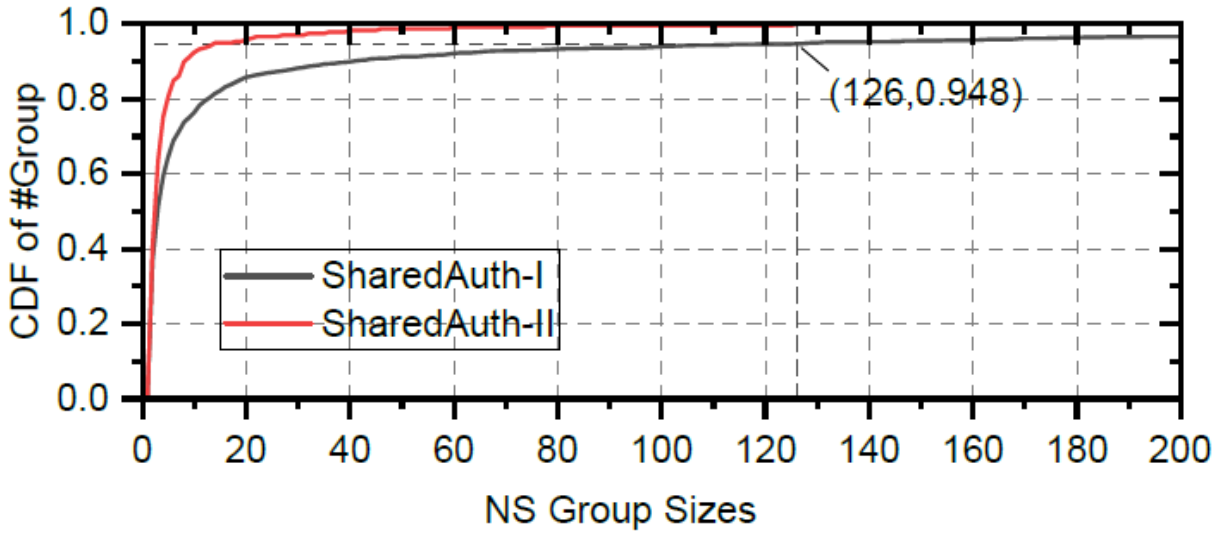
- **Nameserver owner identification**
  - WHOIS, HTTP, domain
- **Cross-entity inspection**
  - free or trial public hosting services



# Shared nameservers are prevalent

XDAuth

- **64,415 shared nameservers**
  - 2,134 SharedAuth-I groups
  - 238 SharedAuth-II groups

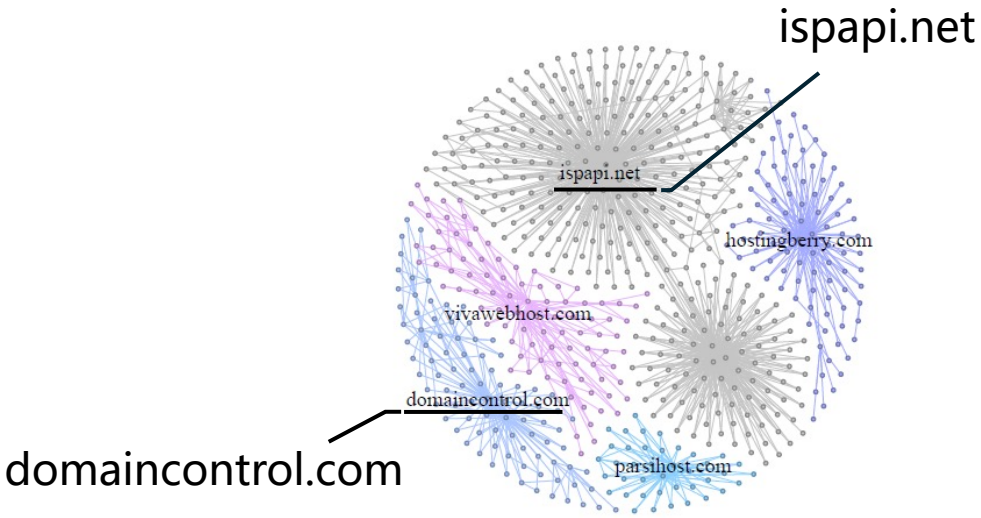



SharedAuth-I displaying larger NS group sizes

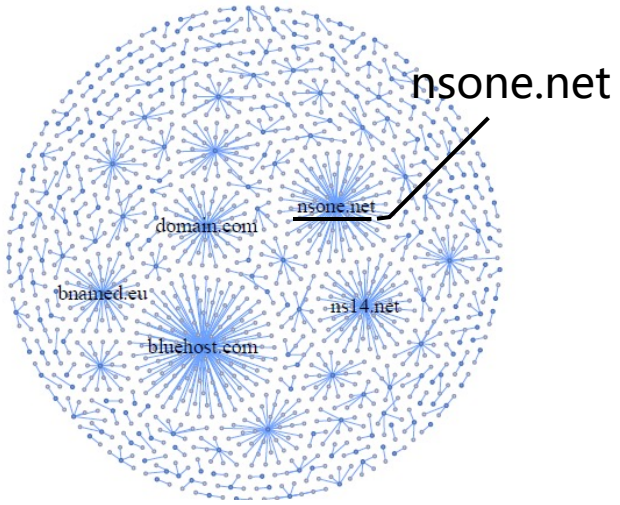
# Different entity tend to share nameserver

XDAuth

- **Clusters of shared nameservers**
  - if any nameserver is vulnerable, it affects all other entities in that group




SharedAuth-I

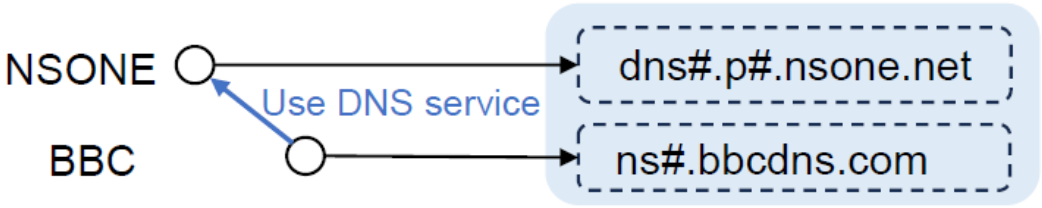



SharedAuth-II

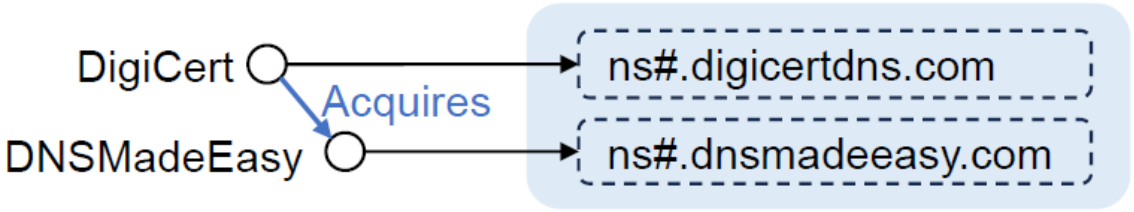
# Different entity tend to share nameserver

XDAuth

- **Clusters of shared nameservers**
- **Common scenarios of shared nameservers**
  - service subscription
  - Different services within a single corporation
  - infrastructures migration
  - Company mergers and acquisitions




Enterprises use public hosting services




Corporate mergers and acquisitions

# Vulnerable Entities

XDAuth

- 12 mainstream DNS hosting providers

NS1. an IBM Company

dnsimple

digicert® DNS Made Easy

HUAWEI

HUAWEI CLOUD

- 125,124 domains of well-known enterprises/organizations

SECTIGO

Zacco

SQUARESPACE

Canon

PORSCHE

BBC

McKESSON

ComLaude

NIKE

# Disclosure & Mitigation

XDAuth

## ❖ Disclosure

- NSONE confirmed and fixed the issues
- McKesson has confirmed the issue and is working on fix

## ❖ Mitigation

- Improve existing NS allocation strategy
- Implementing discontinuation constraints
- Maintaining a global status of domain hosting
- Performing domain ownership verification by other information

# Conclusion

XDAuth

## ❖ New attack surface

- ❖ uncover a new attack surface in the DNS infrastructure: **shared nameservers infrastructure**

## ❖ Novel methodology and findings

- ❖ shared authoritative nameservers are **prevalent**
- ❖ a novel approach to discovering shared nameserver threats
- ❖ demonstrate the risk existing in many DNS hosting provider and enterprises

# Thanks!
# Questions?

Presenter: **Chaoyi Lu**, Tsinghua University
**https://chaoyi.lu**

Author Email:
**zhangyyzyy@nudt.edu.cn**