



DNS Cache Poisoning Attack Reloaded : Revolutions with Side Channels

Video : <http://tinyurl.com/sil765video>

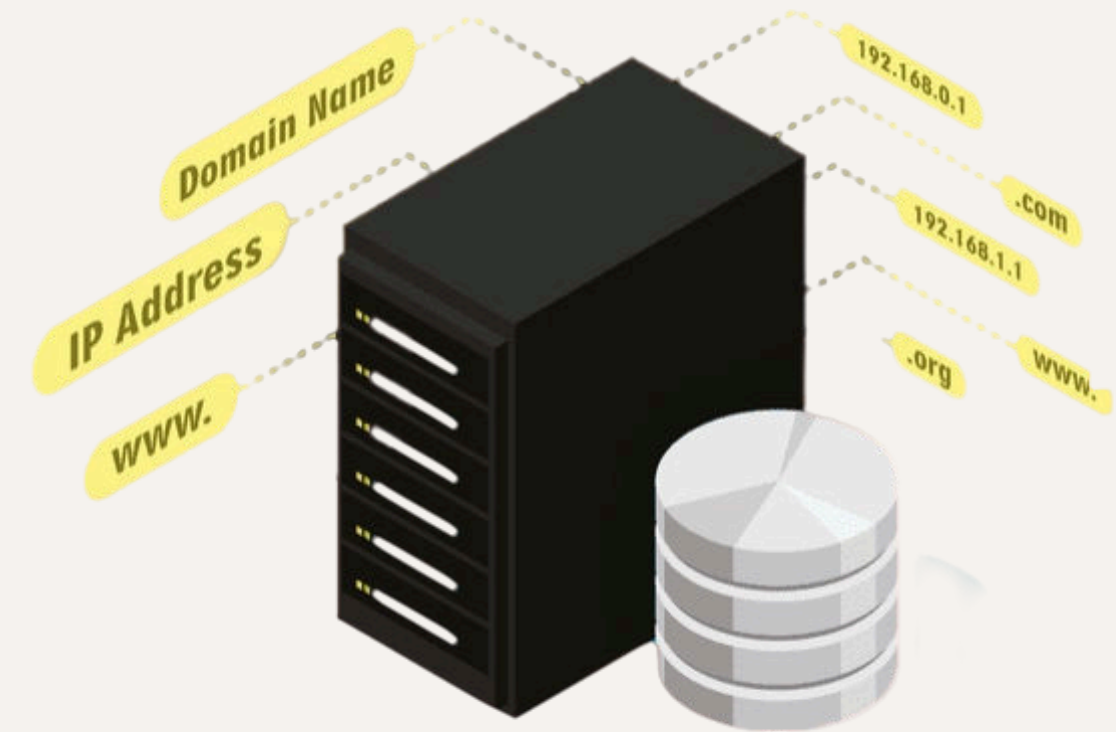


Introduction

An overview of *DNS Cache Poisoning Attack* and its impact on **network security**. This presentation will unmask the threat landscape and provide insights into mitigation strategies.

Paper :

<https://dl.acm.org/doi/pdf/10.1145/3372297.3417280>

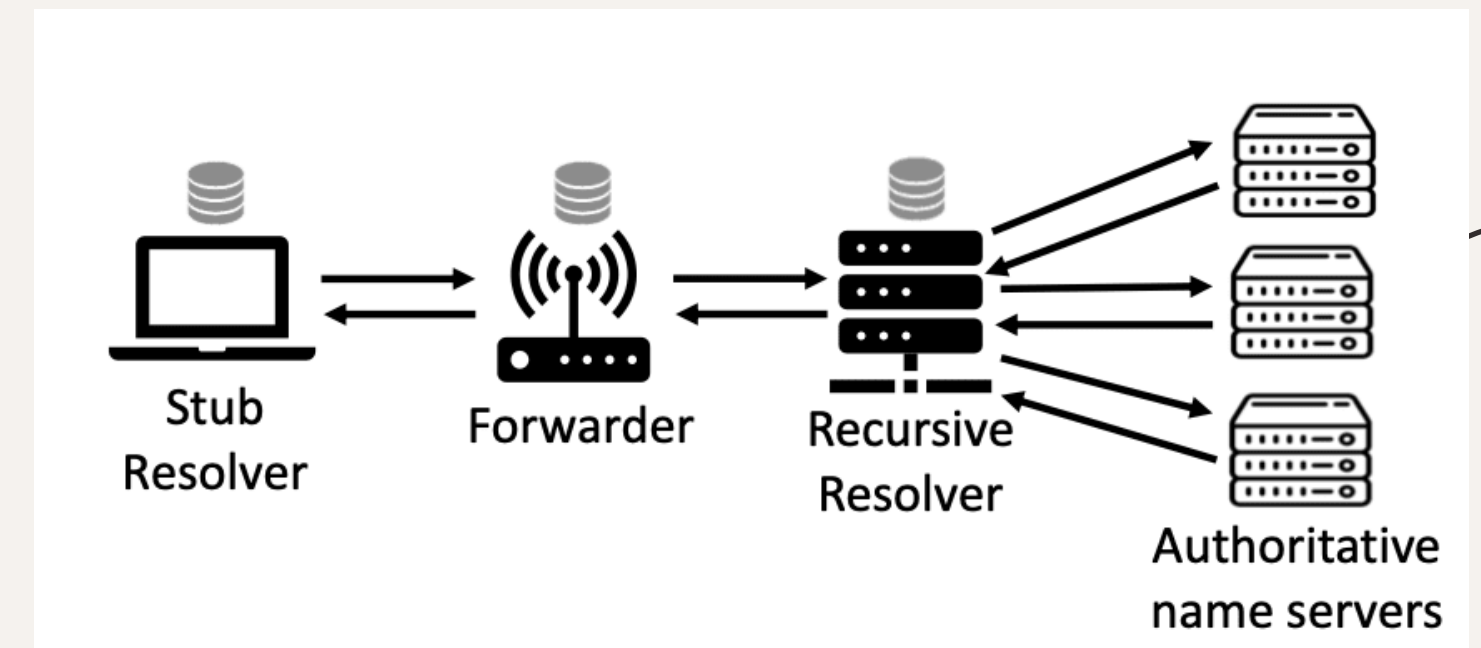


DNS (Domain Name Server)

- A decentralized system translating human-readable domain names into IP addresses for efficient internet communication.
- Works on UDP
- Connects user to authoritative DNS for resolution.

Entities

- source/destination IP
- source/destination port
- transaction ID (TxID) of the query (16 bit long)
- Victim : DNS Resolver, Forwarder





Threat Model


- Off path attack model
- Capability of IP spoofing
- Machine which can trigger request out of forwarder and resolver

Attack workflow

- Inferring source port
- Extending attack window



Defenses

- Randomization of source port
 - Randomization of capitalization of letters in domain names
 - Randomization of the choice of name servers
 - DNSSEC
- 

INFERRING DNS QUERY'S SOURCE PORT

1. ICMP rate limit issue

2. Mitigation

- owns multiple IP addresses
 - multiple addresses using DHCP.
 - IP spoofing
- 

Fast scanning

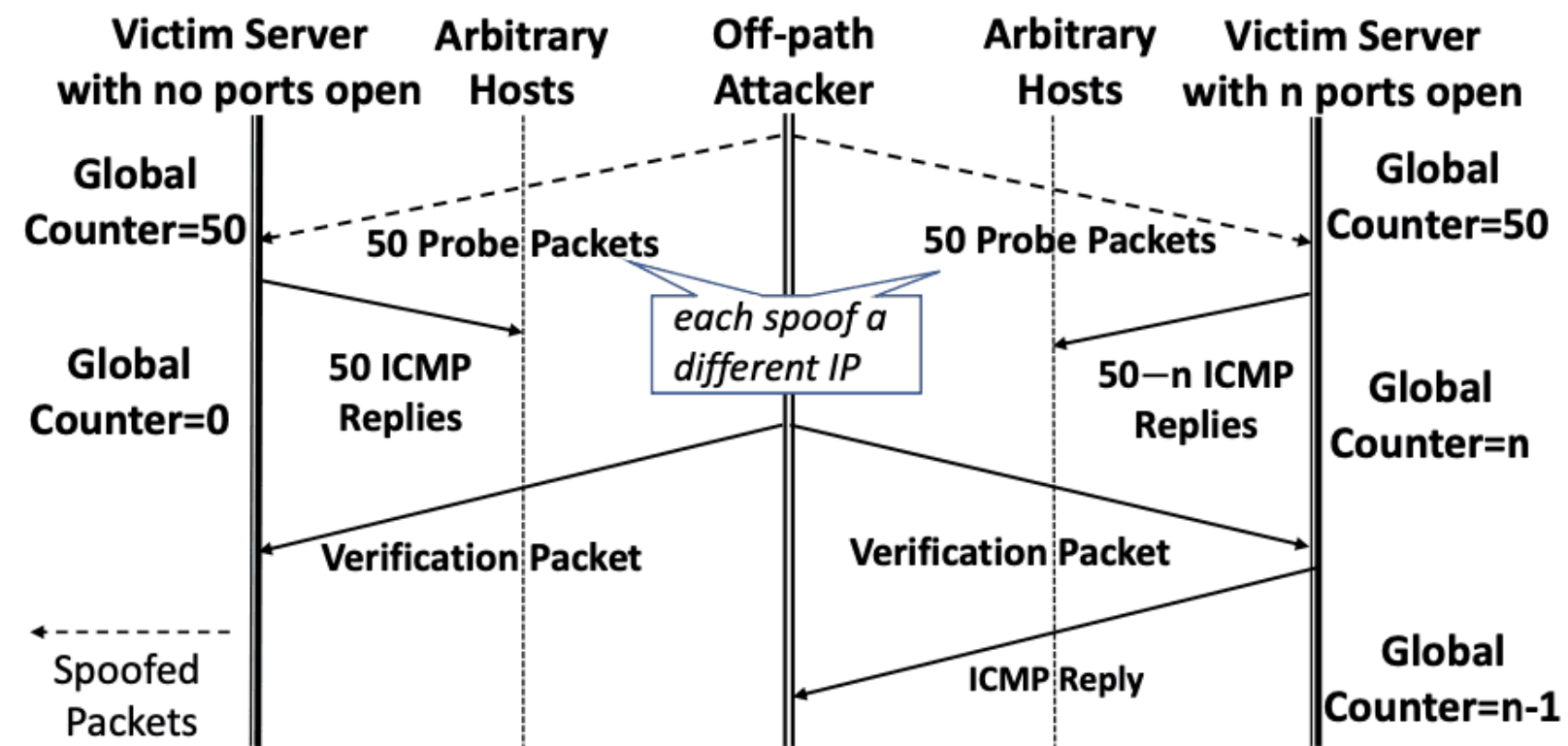


Figure 3: Fast Port Scanning of an Open Source Port

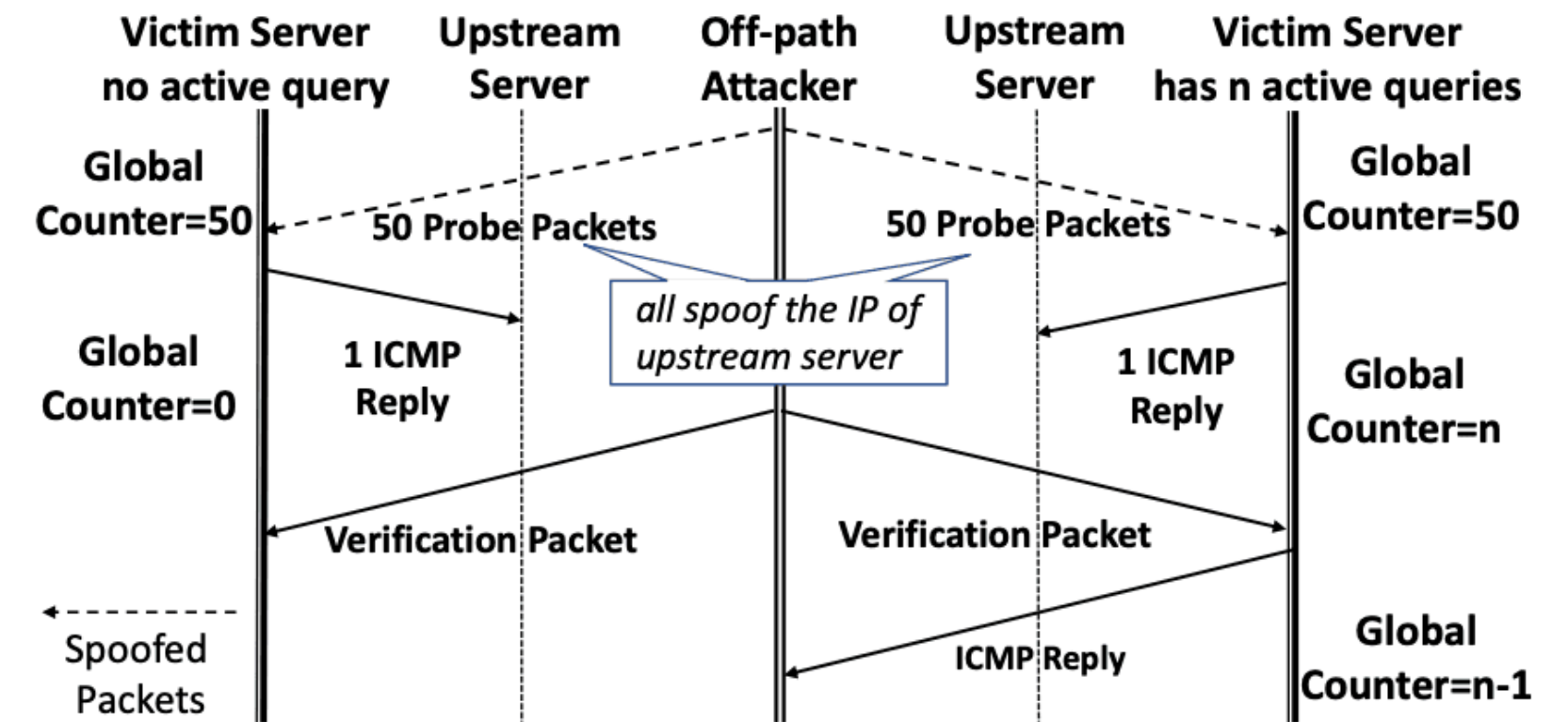


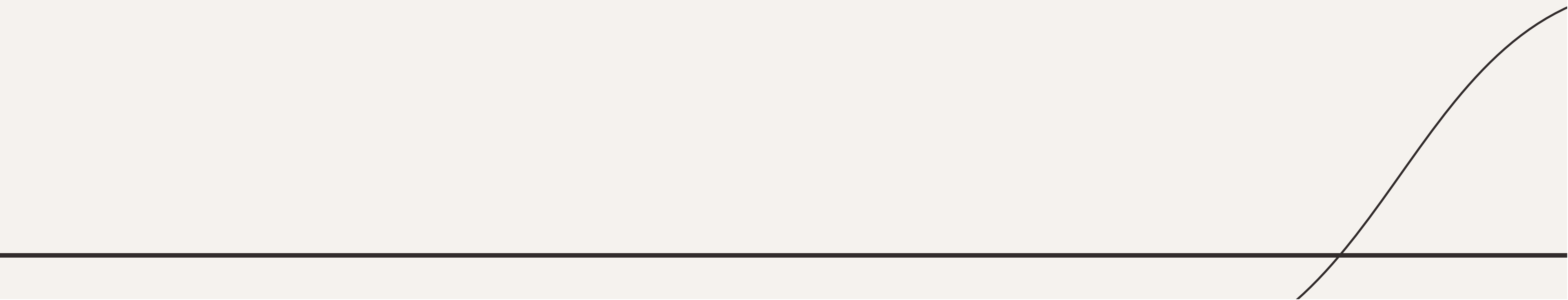
Figure 4: Fast Port Scanning of a Private Source Port

- Binary search
- Handling noises

EXTENDING THE ATTACK WINDOW

- Extending Window in a Forwarder Attack
- Extending Window in a Resolver Attack

PRACTICAL ATTACK CONSIDERATIONS

- Bypassing the TTL of cached records.
 - Timeouts and retransmitted queries.
 - Handling multiple authoritative name servers.
 - Handling multiple backend servers behind DNS resolvers
- 

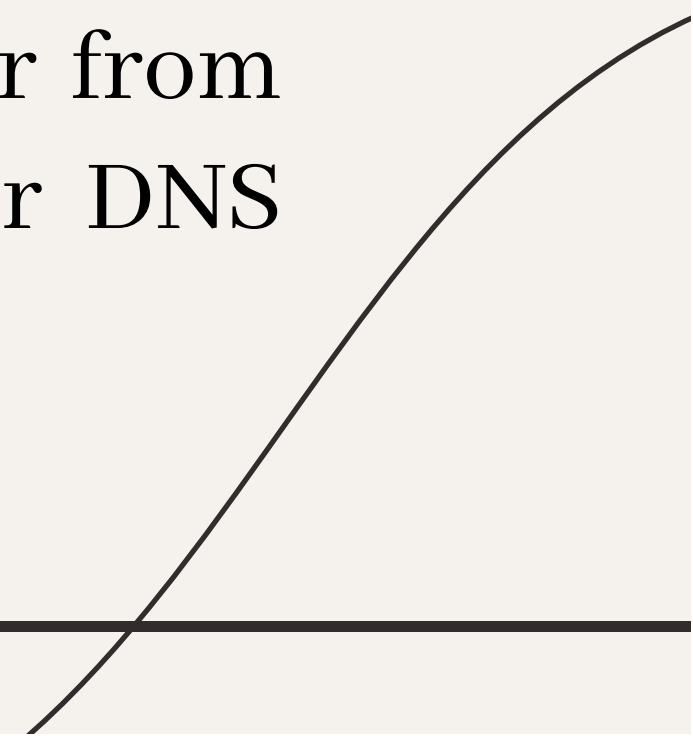
End to end attacks (Experiment)

- Attacking a Forwarder (Home Router)
- Attacking a Production Resolver

Discussion

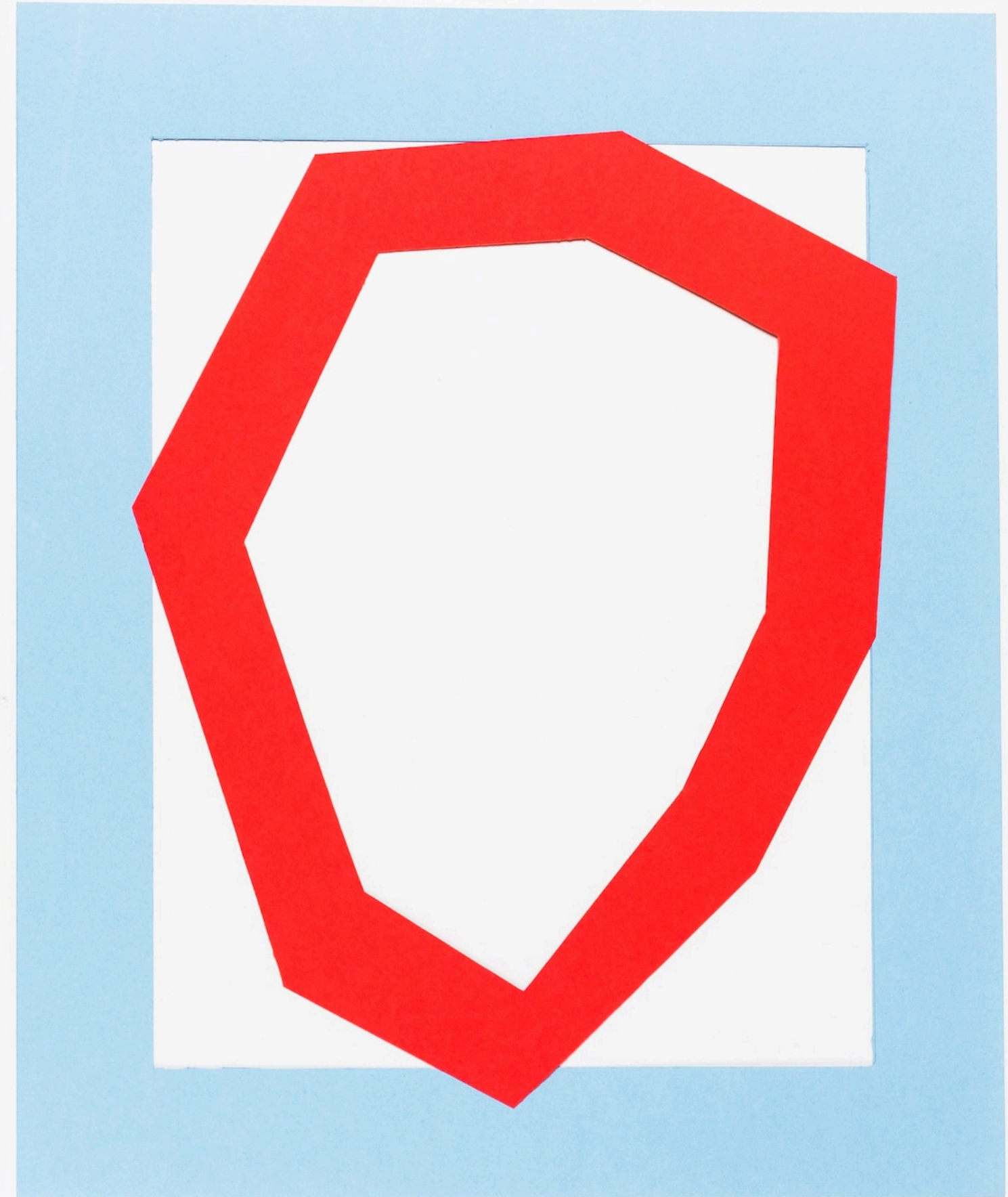
- Attack against Unbound vs. BIND
- UDP source port inference on other operating systems
- Other vulnerable protocols

Defense

- For inferencing source port : The simplest mitigation is to disallow outgoing ICMP replies altogether at the potential cost of losing some network troubleshooting and diagnostic features.
 - For extending attack window : To use RRL to prevent an attacker from muting authoritative name servers easily or set the timeout for DNS queries or employ anycast.
- 

Conclusion

This paper presents a novel and general side channel based on global ICMP rate limit, universally implemented by all modern operating systems. This allows efficient scans of UDP source ports in DNS queries. Combined with techniques to extend the attack window, it leads to a powerful revival of the DNS cache poisoning attack, demonstrated with real-world experiments under realistic server configuration and network conditions. Finally, we suggest practical mitigations that can be used to raise the bar against such attacks.





Thanks!

Gaurav (2021CS10116)
Mayank (2021CS10583)

