DNS Cache Poisoning Attack Reloaded: Revolutions with Side Channels

Keyu Man, Zhiyun Qian, Zhongjie Wang,

Xiaofeng Zheng†, Youjun Huang†, Haixin Duan†

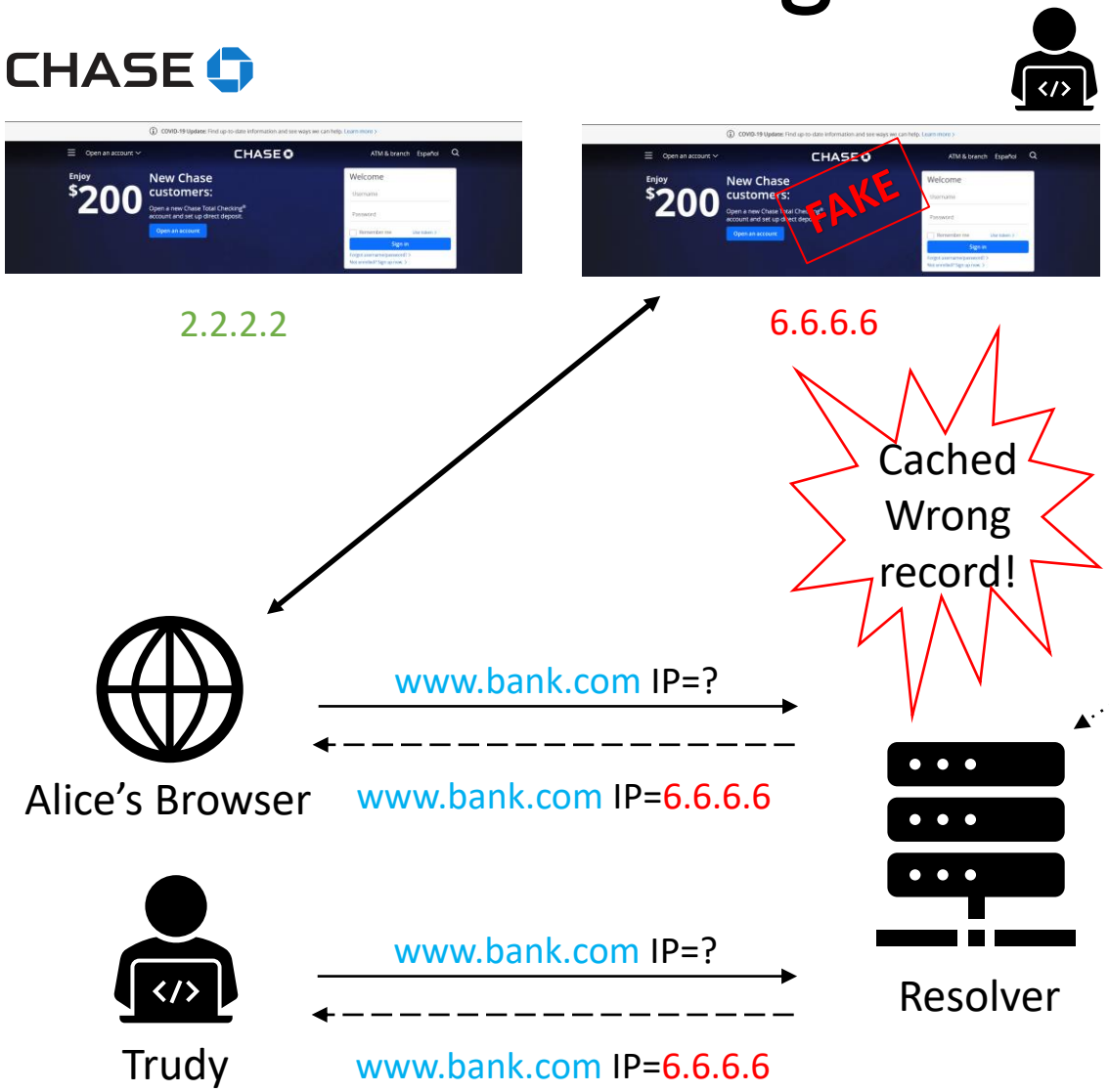
†

UC RIVERSIDE

TSINGHUA UNIVERSITY 1911

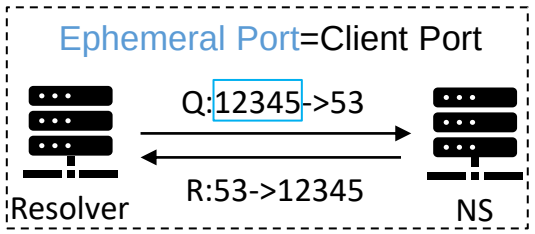
Contents

DNS Cache Poisoning



DNS Cache Poisoning

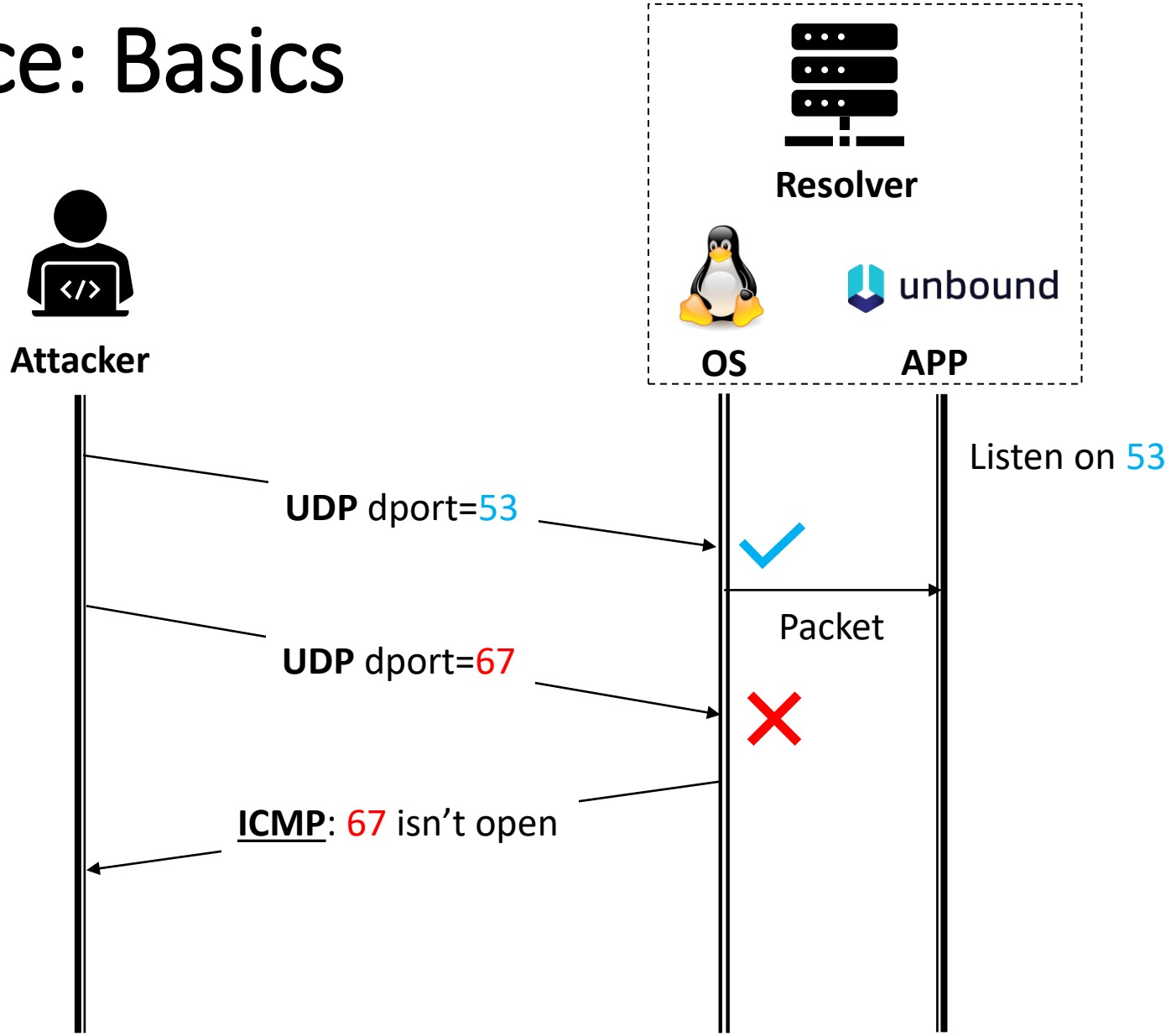
IP Layer	**Src:** 5.6.7.8	
	Dst: *(resolver)*	
UDP Layer	**Src Port:** 53	**Dst Port:**
DNS Layer	**TxID:**	
	Question: www.bank.com A ?	
	Answer: www.bank.com A 6.6.6.6, TTL=**99999**	



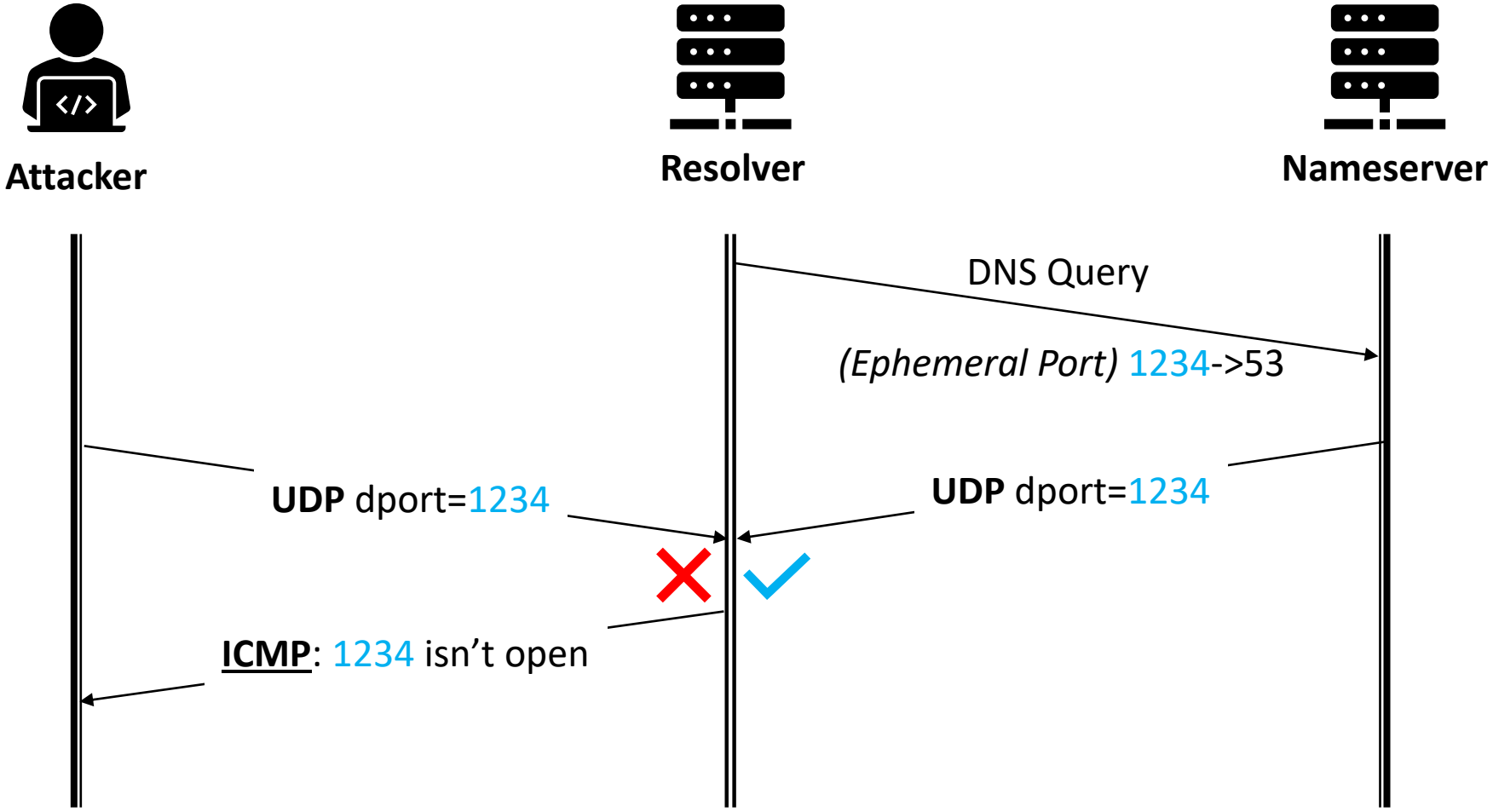
Traditional: $2^{16} \times 2^{16} = 2^{32}$ (Impossible in short time)

Contents

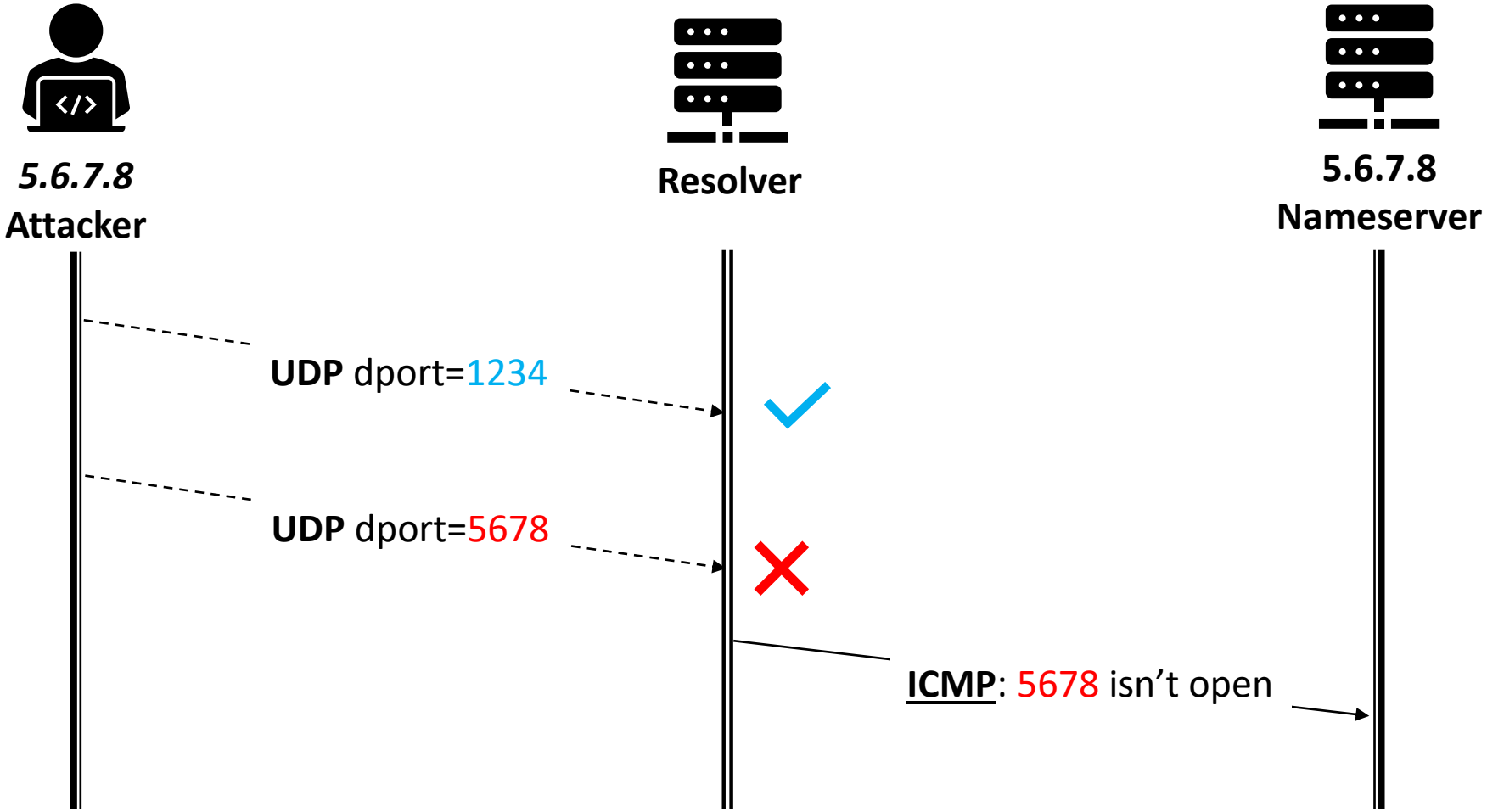
Port Inference: Basics



Port Inference: Ephemeral Ports

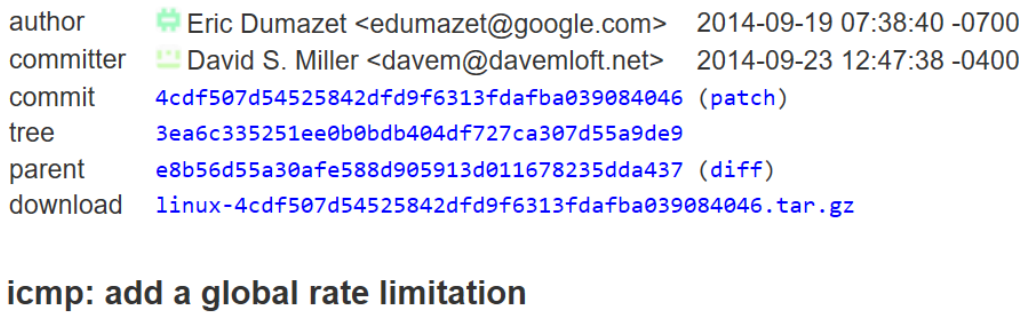


Port Inference: IP Spoofing

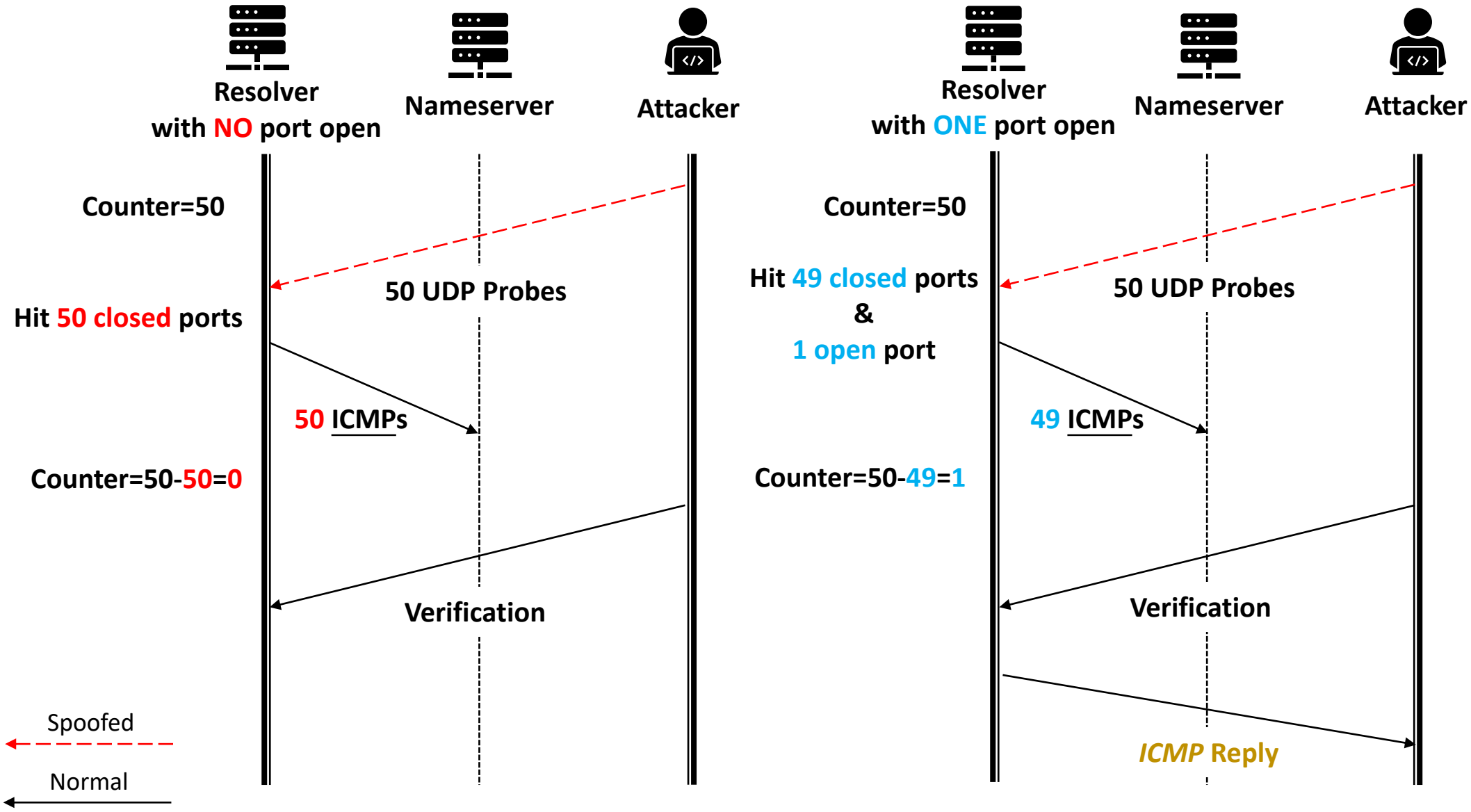


Port Inference:

- ICMP Global Rate Limit:
  - Limit sending rate
  - Shared by all IPs



Port Inference: How It Works



Port Inference: Measurement

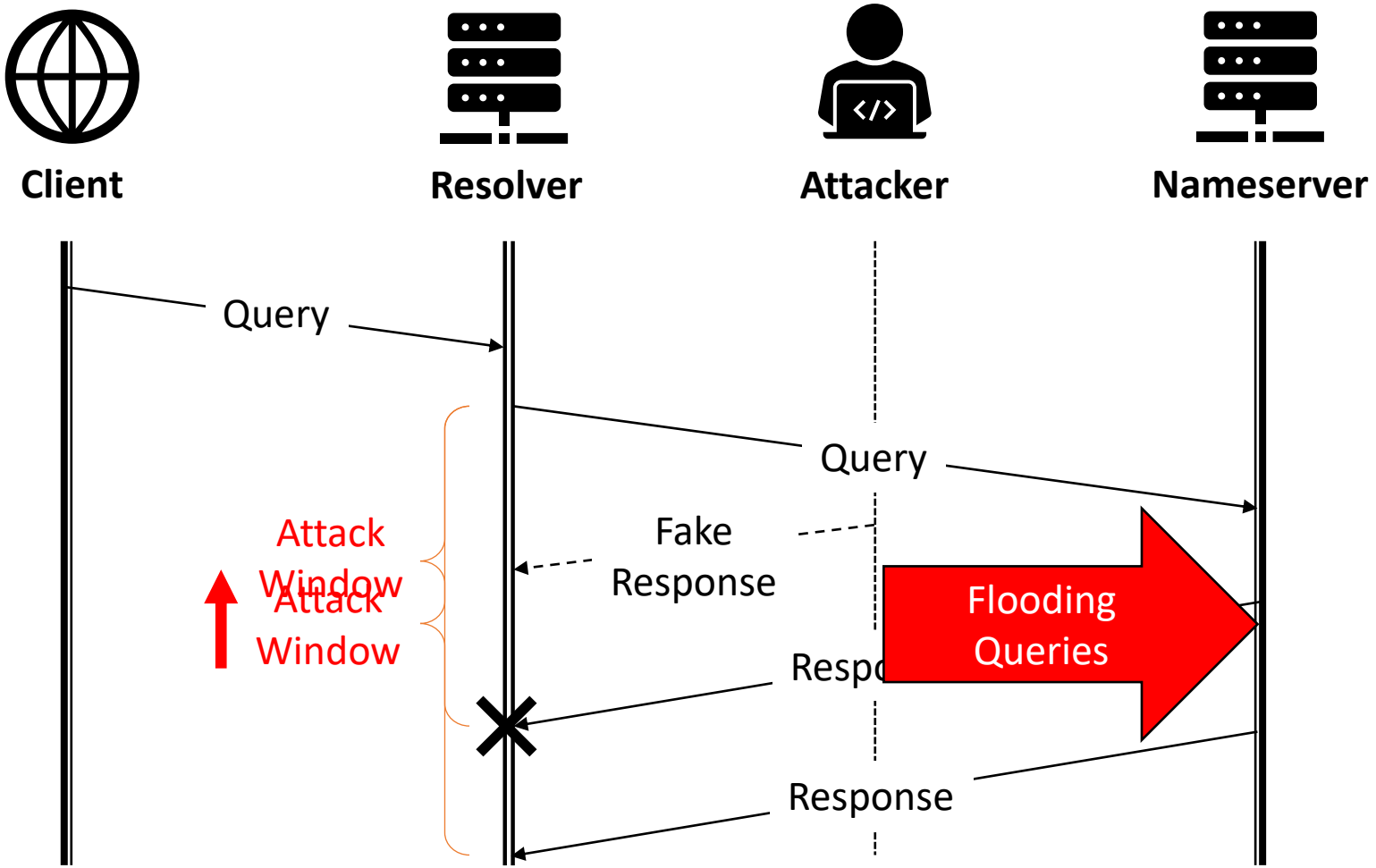
- Open Resolvers:
  - **34%** Vulnerable
- Well-known Public Resolvers:
  - **12**/14 Vulnerable

Google	8.8.8.8
Cloudflare	1.1.1.1
OpenDNS	208.67.222.222
Comodo	8.26.56.26
Dyn	216.146.35.35
Quad9	9.9.9.9
AdGuard	176.103.130.130
CleanBrowsing	185.228.168.168
Neustar	156.154.70.1
Yandex	77.88.8.1
Baidu DNS	180.76.76.76
114 DNS	114.114.114.114
Tencent DNS	119.29.29.29
Ali DNS	223.5.5.5

Contents

- Background
- Overview
- Part I: Infer Ephemeral Port
- Part II: Extend Attack Window
  - Strategy I: Malicious Name Server (Refer to the Paper)
  - Strategy II: Response Rate Limiting
- Our Attacks
- Defenses
- Conclusion
- Disclosure

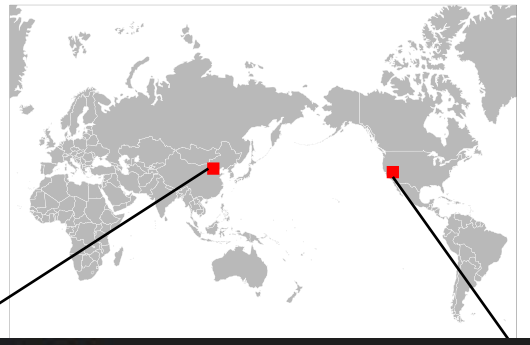
Extend Attack Window



Contents

- Background
- Part I: Infer Ephemeral Port
- Part II: Extend Attack Window
- Our Attacks
  - Forwarder Attack (Refer to the Paper)
  - Resolver Attack
- Defenses
- Conclusion
- Disclosure

Production Resolver Attack



```
          $ dig @          test2.test.xiaofengtest.net +timeout=999

; <<>> DiG 9.11.5-P4-5.1ubuntu2.1-Ubuntu <<>> @          test2.test.xiaofengtest.net +timeout=999
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 7660
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;test2.test.xiaofengtest.net.   IN      A

;; ANSWER SECTION:
test2.test.xiaofengtest.net. 300 IN     A       1.2.3.4

;; AUTHORITY SECTION:
test2.test.xiaofengtest.net. 3534 IN    NS      ns.test2.test.xiaofengtest.net.

;; ADDITIONAL SECTION:
ns.test2.test.xiaofengtest.net. 294 IN  A       54.177.157.64

;; Query time: 172 msec
;; SERVER:          #53(          )
;; WHEN: Thu Apr 02 20:54:05 UTC 2020
;; MSG SIZE  rcvd: 105

          $
```

Attacke

ers

rolled by us)

20ms delay, 3ms jitter, 0.2% loss

Resolver Attack: Results

	Setup					Result	
Attack	# Back Server	# NS	Jitter	Delay	Loss	Total Time	Success Rate
Tsinghua	2	2	3ms	20ms	0.2%	15 mins	5/5

Refer to the paper for more exciting results!

Contents

- Background
- Part I: Infer Ephemeral Port
- Part II: Extend Attack Window
- Our Attacks
- Defenses
- Conclusion
- Disclosure

Defenses

- DNSSEC
- 0x20 encoding
- DNS cookie
  - Only 5% open resolvers deployed
- Disable ICMP port unreachable
- Randomize ICMP global rate limit

Contents

- Background
- Part I: Infer Ephemeral Port
- Part II: Extend Attack Window
- Our Attacks
- Defenses
- Conclusion
- Disclosure

Conclusion

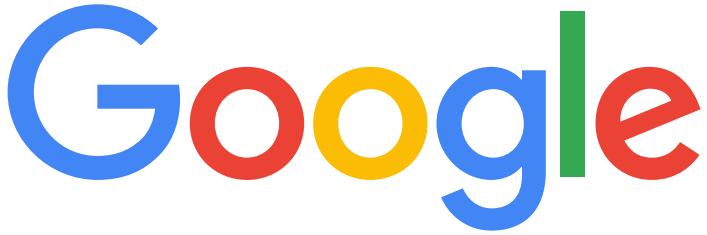
- Side-channel-based UDP port scan.
- Make DNS cache poisoning possible again!
- Real-world attacks.

Contents

- Background
- Part I: Infer Ephemeral Port
- Part II: Extend Attack Window
- Our Attacks
- Defenses
- Conclusion
- Disclosure

Disclosure


THE
LINUX
FOUNDATION


Google


ubuntu


FreeBSD


redhat


CISCO


Microsoft


FORTINET

Thank you!

Q & A

Source code & more interesting projects
https://github.com/seclab-ucr/

Keyu Man
kman001@ucr.edu