DNS Cache Poisoning Attack Reloaded: Revolutions with Side Channels

Keyu Man, Zhiyun Qian, Zhongjie Wang,
Xiaofeng Zheng†, Youjun Huang†, Haixin Duan†
Contents

• Background
  • DNS Cache Poisoning
• Part I: Infer Ephemeral Port
• Part II: Extend Attack Window
• Our Attacks
• Defenses
• Conclusion
• Disclosure
DNS Cache Poisoning

**Alice’s Browser**
- www.bank.com IP=2.2.2.2
- www.bank.com IP=6.6.6.6

**Trudy**
- www.bank.com IP=2.2.2.2
- www.bank.com IP=6.6.6.6
- www.bank.com IP=6.6.6.6

**Resolver**
- www.bank.com IP=?
- www.bank.com IP=6.6.6.6
- www.bank.com IP=2.2.2.2

**bank.com Nameserver (NS)**
- www.bank.com IP=6.6.6.6

**Trudy (Off-path)**
- www.bank.com IP=6.6.6.6
- **Fake**

**Wrong record!**
### DNS Cache Poisoning

<table>
<thead>
<tr>
<th>Layer</th>
<th>Source</th>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Layer</td>
<td><strong>Src:</strong> 5.6.7.8</td>
<td><strong>Dst:</strong> (resolver)</td>
</tr>
<tr>
<td><strong>IP Layer</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>UDP Layer</strong></td>
<td><strong>Src Port:</strong> 53</td>
<td><strong>Dst Port:</strong></td>
</tr>
<tr>
<td><strong>DNS Layer</strong></td>
<td><strong>TxID:</strong></td>
<td><strong>Question:</strong> <a href="http://www.bank.com">www.bank.com</a> A ?</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Answer:</strong> <a href="http://www.bank.com">www.bank.com</a> A 6.6.6.6, TTL=99999</td>
</tr>
</tbody>
</table>

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

**Ephemeral Port = Client Port**

- Q: [12345] -> 53
- R: 53 -> [12345]

**Resolver**

- www.bank.com IP=6.6.6.6
- 5.6.7.8 (Trudy, Off-path)
Contents

• Background

• Part I: Infer Ephemeral Port
  • Method I: Direct Scan (Refer to the Paper)
  • Method II: Side-channel-based Scan

• Part II: Extend Attack Window

• Our Attacks

• Defenses

• Conclusion

• Disclosure
Port Inference: Basics

**Attacker**

- **UDP dport=53**
- **UDP dport=67**
- **ICMP: 67 isn’t open**

**Resolver**

**OS**

**APP**

Packet

- **Listen on 53**

Orientation: Vertical
Port Inference: Ephemeral Ports

Attacker

Resolver

Nameserver

UDP dport=1234

ICMP: 1234 isn’t open

UDP dport=1234

DNS Query

(Ephemeral Port) 1234->53
Port Inference: IP Spoofing

5.6.7.8
Attacker

5.6.7.8
Nameserver

UDP dport=1234

UDP dport=5678

Resolver

ICMP: 5678 isn’t open
Port Inference:

- ICMP Global Rate Limit:
  - Limit sending rate
  - Shared by all IPs
Port Inference: How It Works

Resolver with NO port open

Nameserver

Attacker

Counter=50

Hit 50 closed ports

Counter=50 - 50 = 0

50 UDP Probes

50 ICMPs

Verification

Spoofed

Normal

Nameserver

Attacker

Resolver with ONE port open

Counter=50

Hit 49 closed ports & 1 open port

Counter=50 - 49 = 1

50 UDP Probes

49 ICMPs

Verification

ICMP Reply
Port Inference: Measurement

- Open Resolvers:
  - **34%** Vulnerable

- Well-known Public Resolvers:
  - **12/14** Vulnerable

<table>
<thead>
<tr>
<th>Resolver</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google</td>
<td>8.8.8.8</td>
</tr>
<tr>
<td>Cloudflare</td>
<td>1.1.1.1</td>
</tr>
<tr>
<td>OpenDNS</td>
<td>208.67.222.222</td>
</tr>
<tr>
<td>Comodo</td>
<td>8.26.56.26</td>
</tr>
<tr>
<td>Dyn</td>
<td>216.146.35.35</td>
</tr>
<tr>
<td>Quad9</td>
<td>9.9.9.9</td>
</tr>
<tr>
<td>AdGuard</td>
<td>176.103.130.130</td>
</tr>
<tr>
<td>CleanBrowsing</td>
<td>185.228.168.168</td>
</tr>
<tr>
<td>Neustar</td>
<td>156.154.70.1</td>
</tr>
<tr>
<td>Yandex</td>
<td>77.88.8.1</td>
</tr>
<tr>
<td>Baidu DNS</td>
<td>180.76.76.76</td>
</tr>
<tr>
<td>114 DNS</td>
<td>114.114.114.114</td>
</tr>
<tr>
<td>Tencent DNS</td>
<td>119.29.29.29</td>
</tr>
<tr>
<td>Ali DNS</td>
<td>223.5.5.5</td>
</tr>
</tbody>
</table>
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

RRL: 18% Deployed

Client → Resolver → Attacker → Nameserver

Query → Fake Response → Flooding Queries

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
20ms delay, 3ms jitter, 0.2% loss
```
## Resolver Attack: Results

<table>
<thead>
<tr>
<th>Attack</th>
<th># Back Server</th>
<th># NS</th>
<th>Jitter</th>
<th>Delay</th>
<th>Loss</th>
<th>Total Time</th>
<th>Success Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tsinghua</td>
<td>2</td>
<td>2</td>
<td>3ms</td>
<td>20ms</td>
<td>0.2%</td>
<td>15 mins</td>
<td>5/5</td>
</tr>
</tbody>
</table>

*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
Thank you!

Q & A

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

Keyu Man
kman001@ucr.edu