Identifying Load-Balanced Backends

Ian Rodney
Why does it matter?

• Targeted DDoS
• Service degradation
Load Balancers

- Terminate & regenerate
  
- Pass through

- Hashing–IP/Port
Side Channels

• Information leaks around shared state
• Well studied
• Setup:
IPID Mechanism

- Unique fragment ID
  - 16-bit field in IPv4

- Counter types:
  - Global
  - Per-Destination
  - Hybrid (2048 counters)

ID field is supposed to be unique per IP packet.

One easy way to do this: increment it each time system sends a new packet.
IPID

• Global Counter
• Per-Dest
• Hybrid

Side Channel

• Covered in lecture!
IPID

• Global Counter
• Per-Dest
• Hybrid

Side Channel

• Pretty hard to defeat
• But there is a way
IPID

- Global Counter
- Per-Dest
- Hybrid

Source: IPv6 Test; S/A
RST, IPID: \( n \)

Source: Victim; S/A
Source: IPv6 Test; S/A
RST, IPID: \( n+1 \) or \( n+2 \)

Global Counter with found IPv6 Address

Xu 2018
**Timestamps**

- Systems have a unique clock drift

<table>
<thead>
<tr>
<th></th>
<th>TCP</th>
<th>ICMP</th>
<th>HTTP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resolution</td>
<td>1Hz – 1 kHz</td>
<td>1kHz</td>
<td>1Hz</td>
</tr>
<tr>
<td>Constant Drift</td>
<td>Yes</td>
<td>NTP adjusted</td>
<td>Yes</td>
</tr>
</tbody>
</table>

• Is 1Hz too low?

NTP removes offset

Shared State  Mechanisms

- Fragment reassembly buffer
- TCP SYN Cache
- Challenge ACK rate limit
Rate-Limit Mechanism

- Challenge ACK rate limit
  - SYN or RST variants
Rate-Limit Mechanism

- Challenge ACK rate limit
  - SYN or RST variants
Rate-Limit

- Infer presence of connection

Cao & Et. Al 2016
Rate-Limit

- Infer presence of connection
**Buffer**

- Fragment buffer & per-destination IPID
- *subtle*

**Side Channel**

Source: A, Frag
Source: U, Frag
Source: V, Full

![Diagram with IPID values](U, IPID: 10
A, IPID: 80
U, IPID: 20
A, IPID: 90)

Cao & Et. Al 2016
Buffer

- Fragment buffer & per-destination IPID

- subtle

Side Channel

Source: A, New Frag

Internet

Victim

Attacker

User

U, IPID: 10
A, IPID: 80
A, IPID: 100
A, IPID: 90

Zhang 2018
Buffer

- Fragment buffer & per-destination IPID

- subtle

Side Channel

Source: A, Remainders: 80, 90, 100

Reply for 80, 90, 100

U, IPID: 10
A, IPID: 80
A, IPID: 100
A, IPID: 90
SYN Cache

- Fill up cache (SYN cookies)
  - Different source ports

Side Channel

Zhang & Et. Al 2015

V, SYN
V, SYN

Source: V

SYN

Patsy

 Exists: RST

S/A

Attack

Internet

Victim

Zhang & Et. Al 2015
SYN Cache

- Fill up cache (SYN cookies)
  - Different source ports

Zhang & Et. Al 2015
How to leverage?

- **IPID:**
  - Global --> straight forward
  - Per-Dest/2048 --> impossible/hard

- Timestamps --> straight forward

- Shared State --> overwhelm and check
My contributions

• Check for side-channel presence
  • Alexa Top 1000
My contributions

• Check for side-channel presence
  • Alexa Top 1000

• ICMP/TCP/HTTP timestamps

• TCP traceroute (termination location)
Tools

• Scapy
  • Raw pcaps
  • Packet manipulation
• Requests
  • HTTP
• Ray
  • Distributed programming (scanning)
Results (a few)

- 986 responses
  - 98% had TCP responses
    - 60% had TCP timestamps
  - 85% had HTTP responses
  - 0 ICMP
Results (a few)
Results (a few)
Results (a few)

ICMP

TCP

TCP terminated first
Terminated at same place
ICMP terminated first
Results (a few)
Results (a few)

ICMP
TCP

![Diagram showing the comparison between ICMP and TCP with a bar chart illustrating additional hops for TCP.]
Results (a few)
Lessons Learned

- Don't underestimate the kernel
Lessons Learned

• Don't underestimate the kernel
• ISPs can be annoying
Lessons Learned

• Don't underestimate the kernel
• ISPs can be annoying
• I don't get IPv6
  • Google IPv6 DNS + IPv6 ISP support = No connection?!
Experiments

- Existence of Challenge ACKs
- IPv6 reachability
- HTTP timestamp analysis

Next Steps
Validation

Next Steps

• Simple GCP Load Balanced Web Server
  • Easy ground-truth

• In-the-wild validation

```ini
# Response Headers
accept-ranges: bytes
age: 67630
cache-control: private, s-maxage=0, max-age=0, must-revalidate
content-encoding: gzip
content-language: en
content-length: 22795
content-type: text/html; charset=UTF-8
date: Thu, 23 Apr 2020 13:26:38 GMT
last-modified: Sat, 18 Apr 2020 19:06:18 GMT
server: mw1325.eqiad.wmnet
```
Questions?

Thanks for listening!