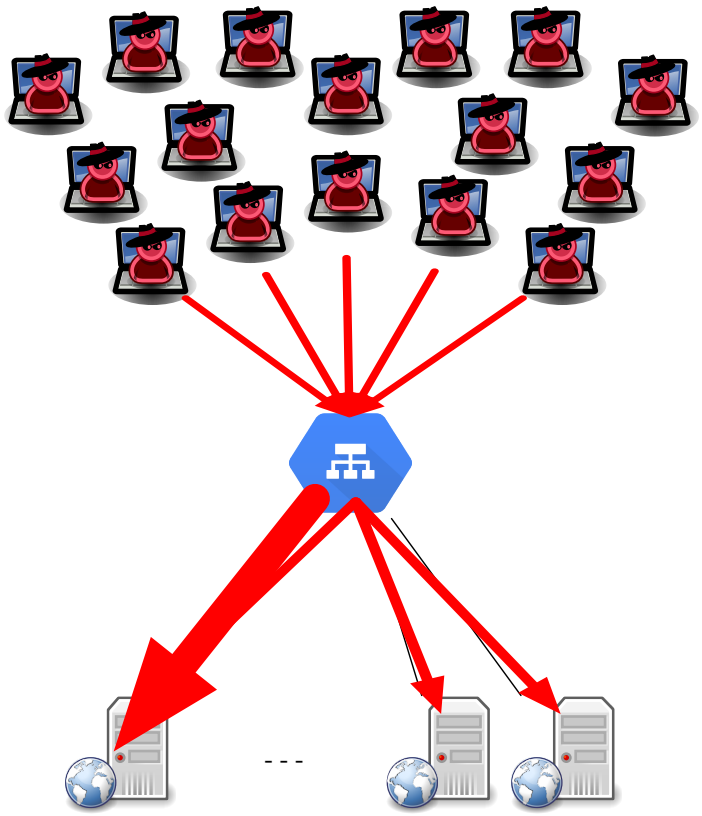
Identifying Load-Balanced Backends

Ian Rodney

Why does it matter?

- Targeted DDoS
- Service degradation



Load Balancers

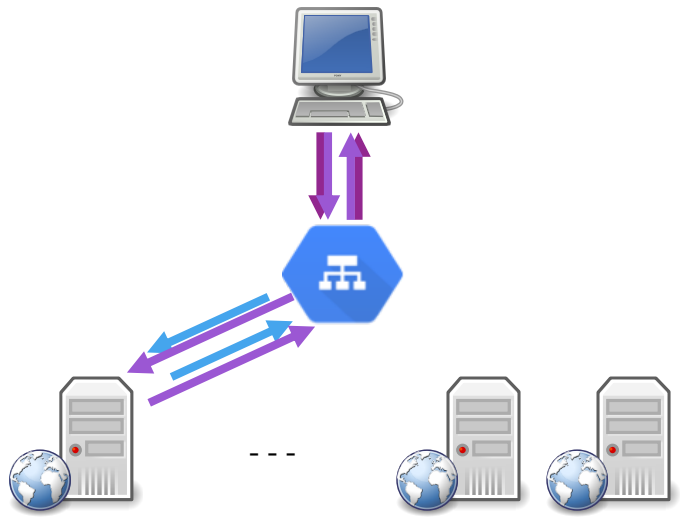
- Terminate & regenerate

  :(

- Pass through

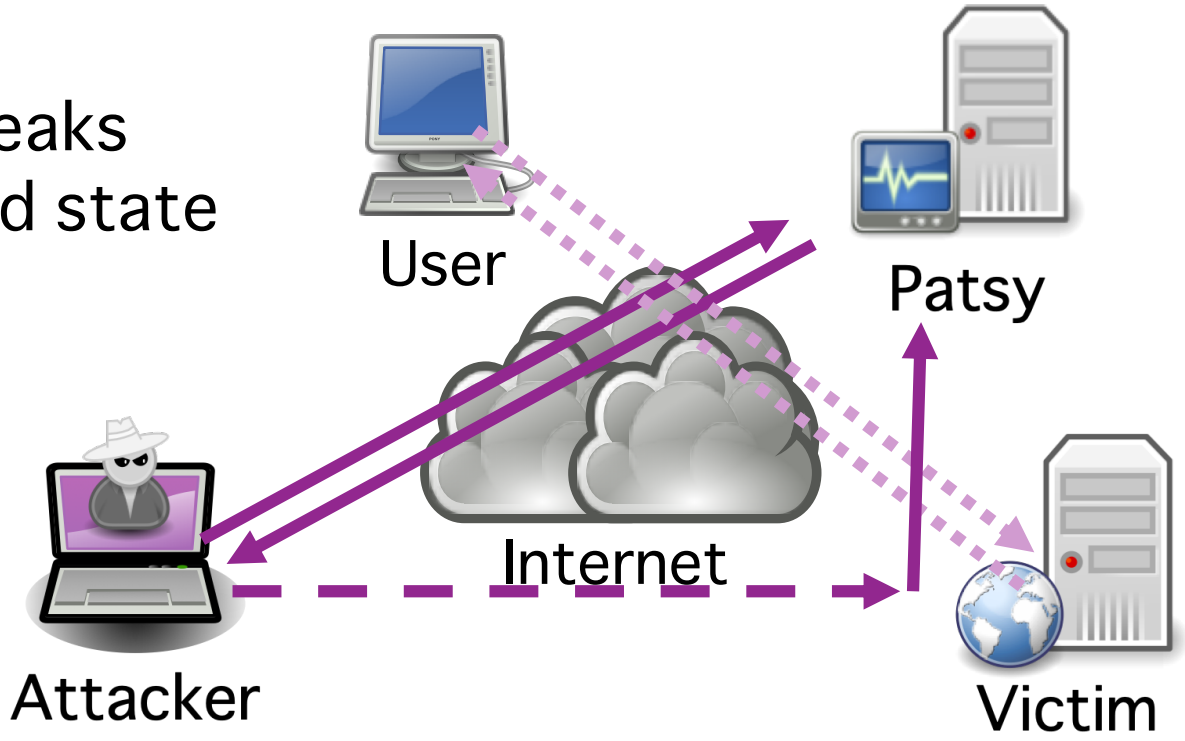
  :)

- Hashing–IP/Port



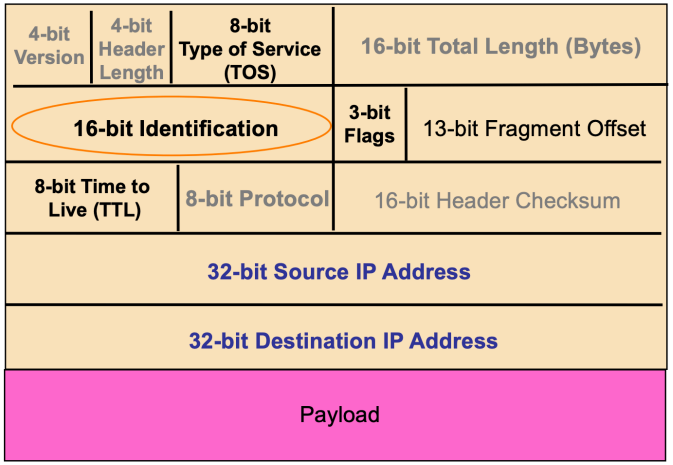
Side Channels

- Information leaks around shared state
- Well studied
- Setup:



IPID Mechanism

- Unique fragment ID
  - 16-bit field in IPv4



ID field is supposed to be unique per IP packet.

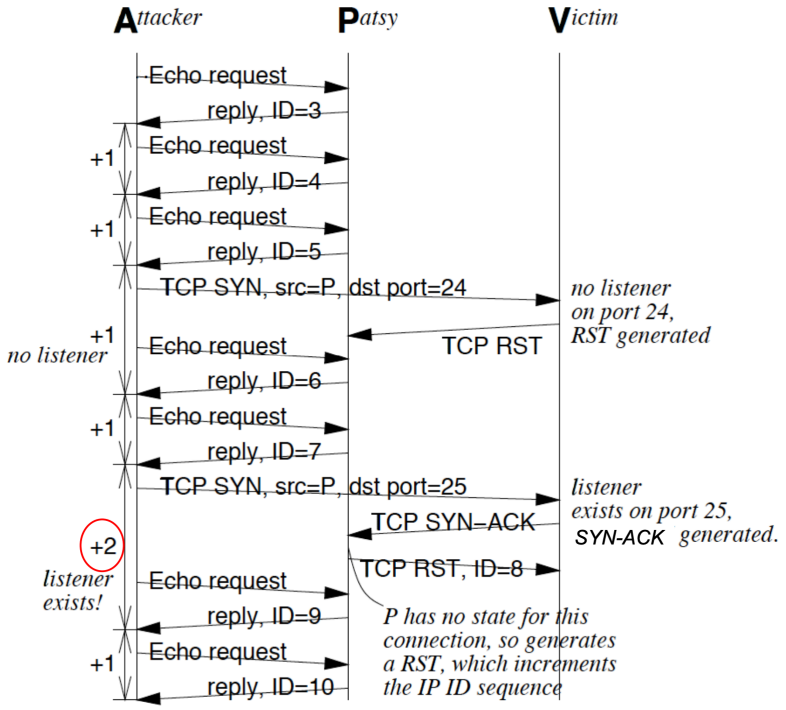
One easy way to do this: **increment** it each time system sends a new packet.

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

IPID Side Channel

- Global Counter
- Per-Dest
- Hybrid

- Covered in lecture!



IPID

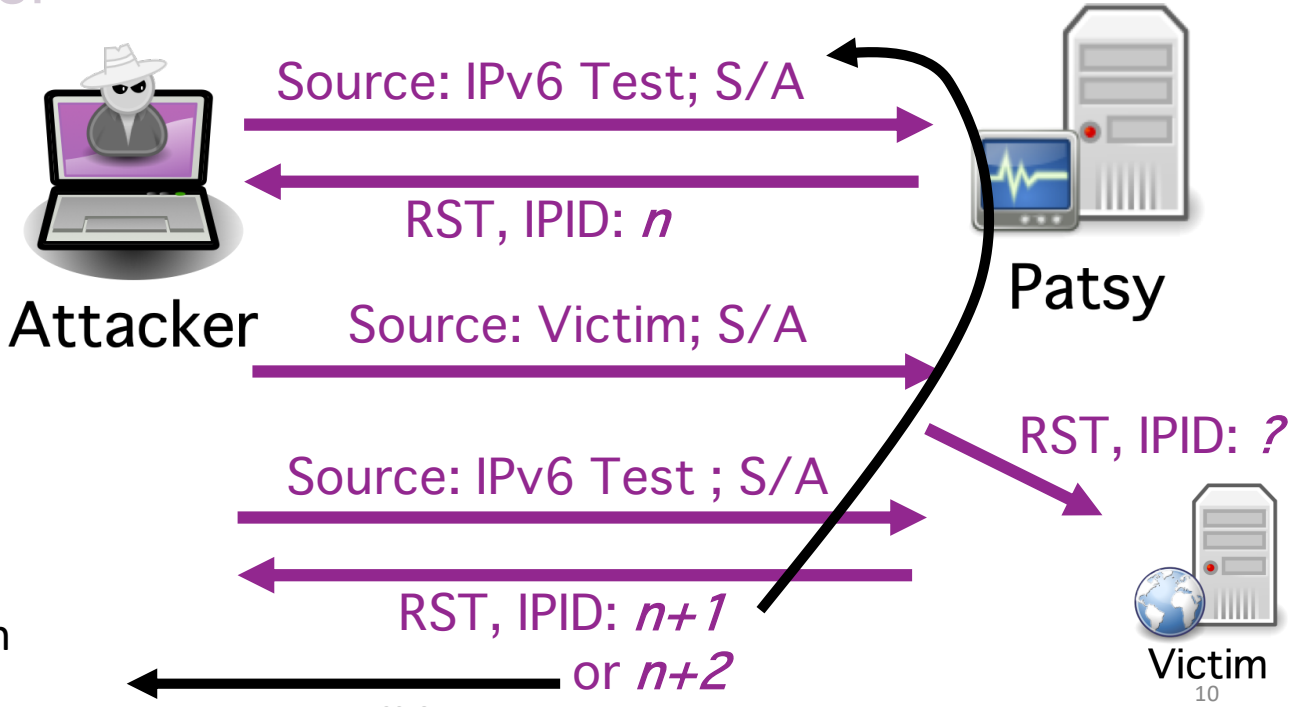
Side Channel

- Global Counter
- Per-Dest
- Hybrid

- Pretty hard to defeat
- But there is a way

IPID Side Channel

- Global Counter
- Per-Dest
- Hybrid



Global Counter with found IPv6 Address

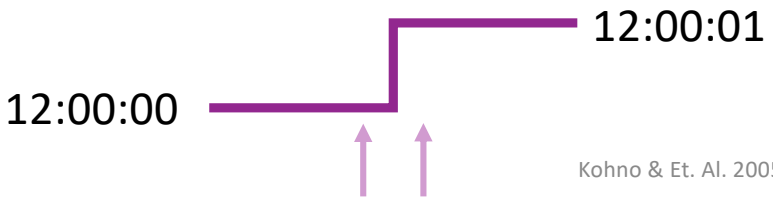
Timestamps Mechanisms

- Systems have a unique clock drift

	TCP	ICMP	HTTP
Resolution	1Hz – 1 kHz	1kHz	1Hz
Constant Drift	Yes	NTP adjusted	Yes

NTP removes offset

- Is 1Hz too low?

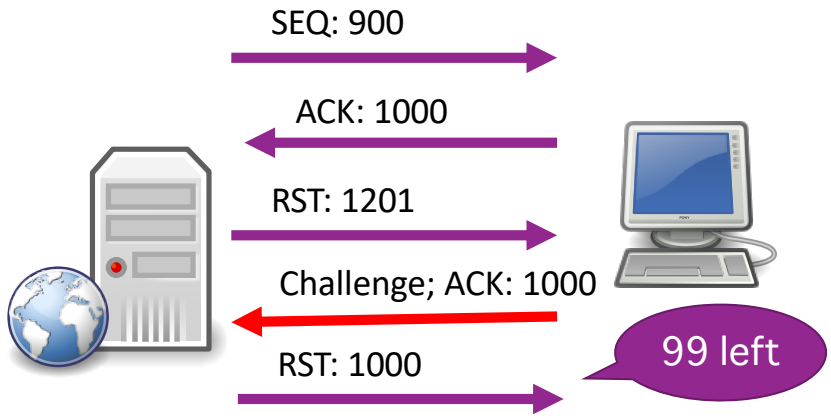


Shared State Mechanisms

- Fragment reassembly buffer
- TCP SYN Cache
- Challenge ACK rate limit

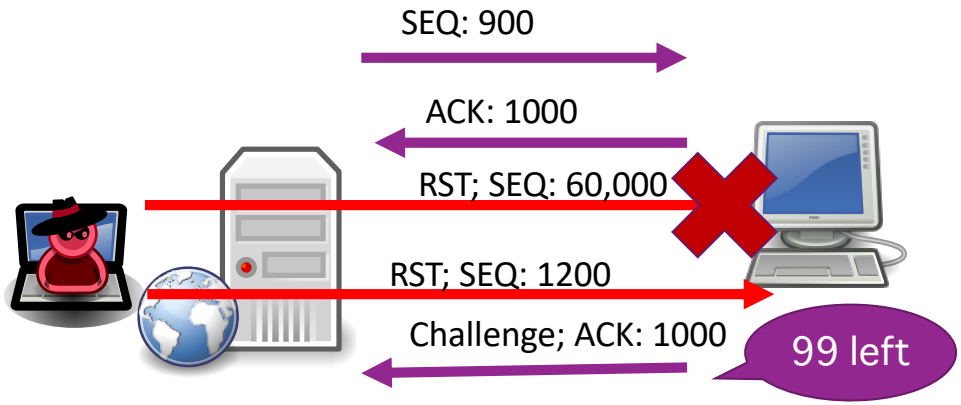
Rate-Limit Mechanism

- Challenge ACK rate limit
  - SYN or RST variants



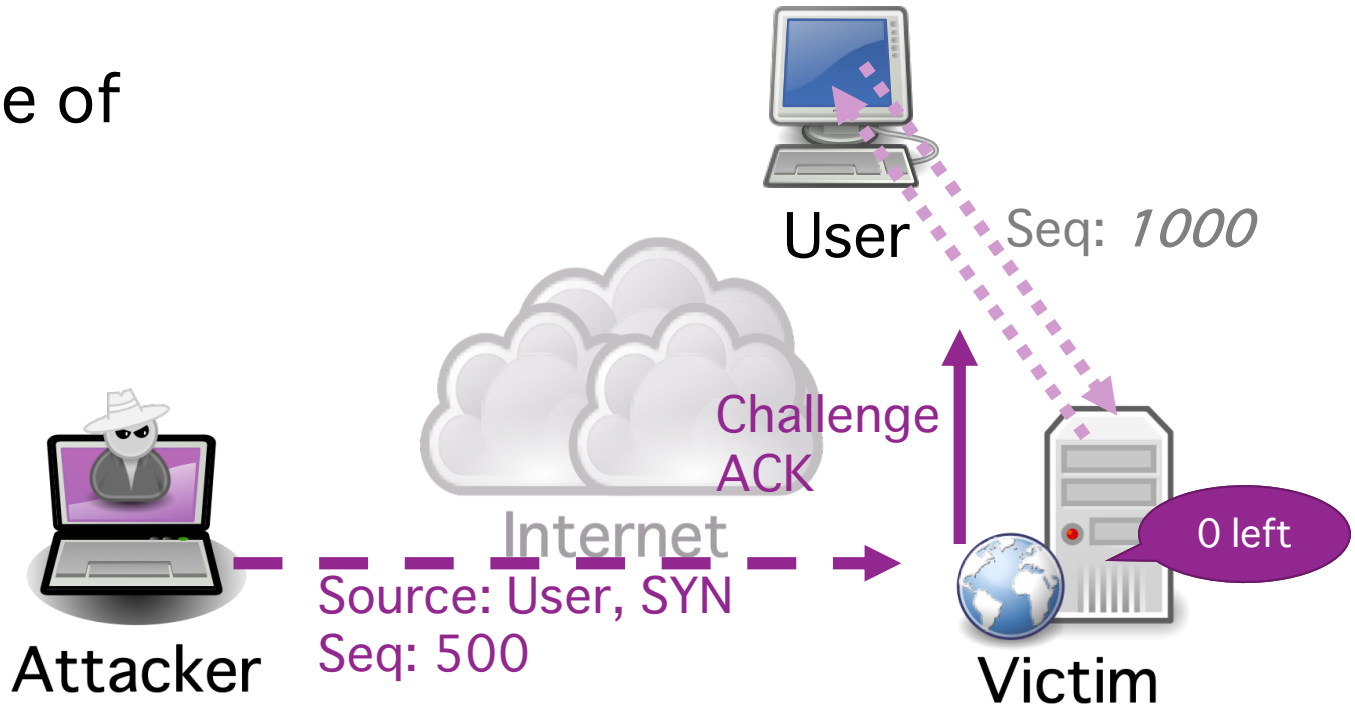
Rate-Limit Mechanism

- Challenge ACK rate limit
  - SYN or RST variants



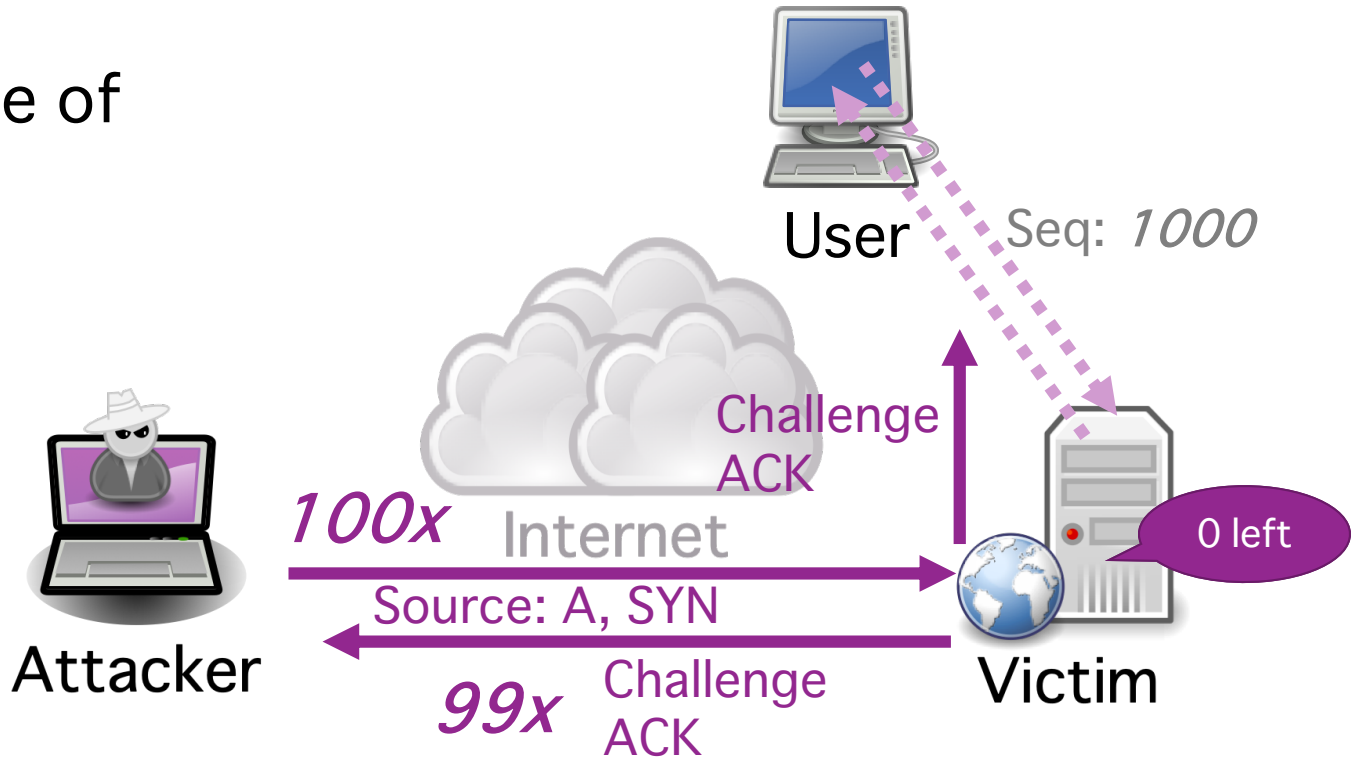
Rate-Limit Side Channel

- Infer presence of connection



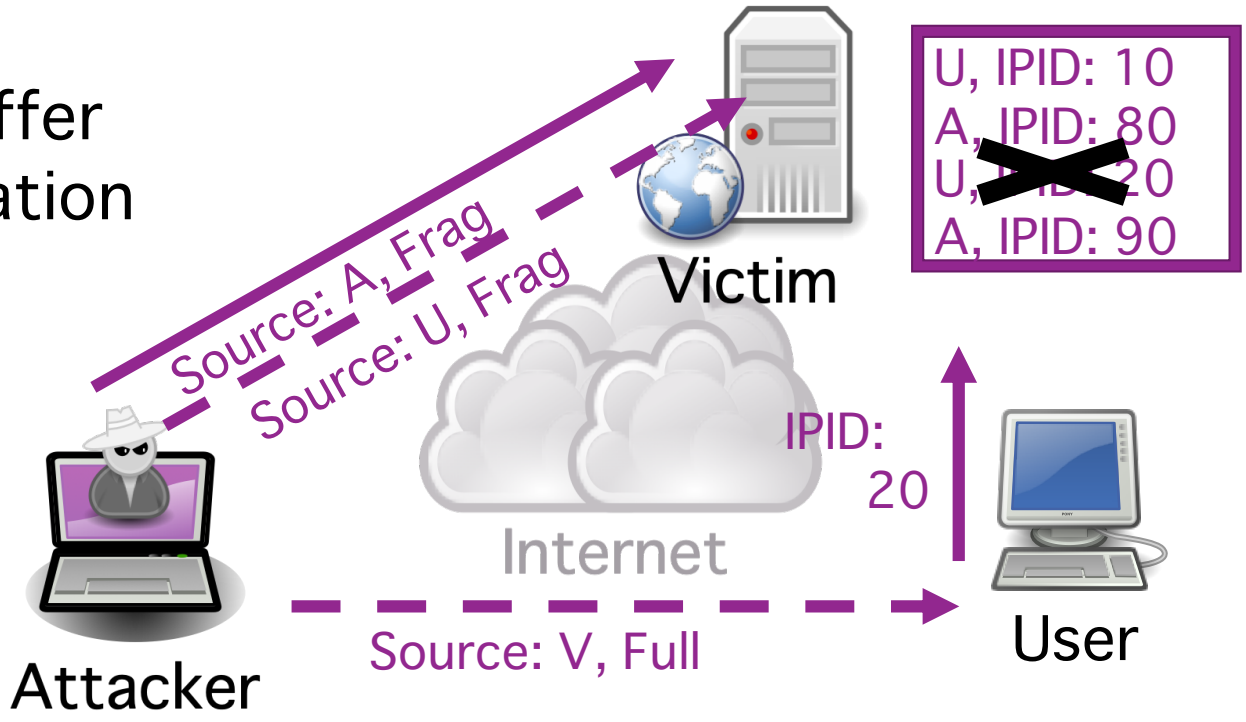
Rate-Limit Side Channel

- Infer presence of connection



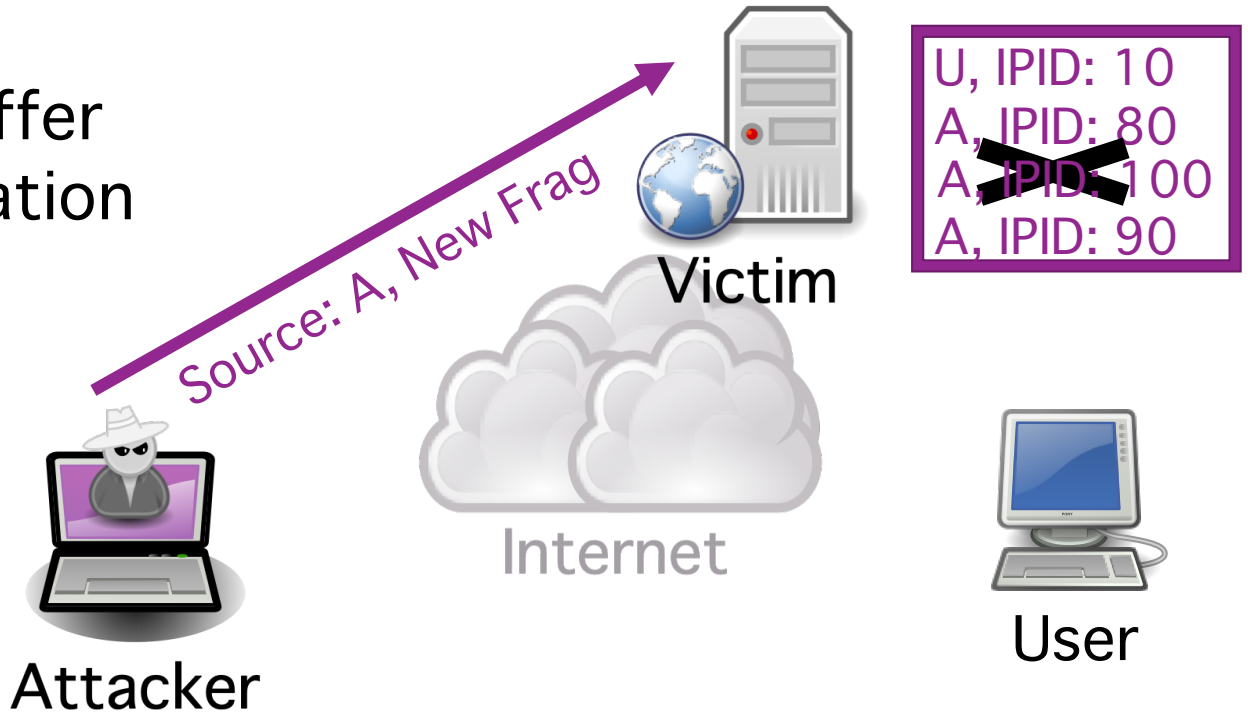
Buffer Side Channel

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



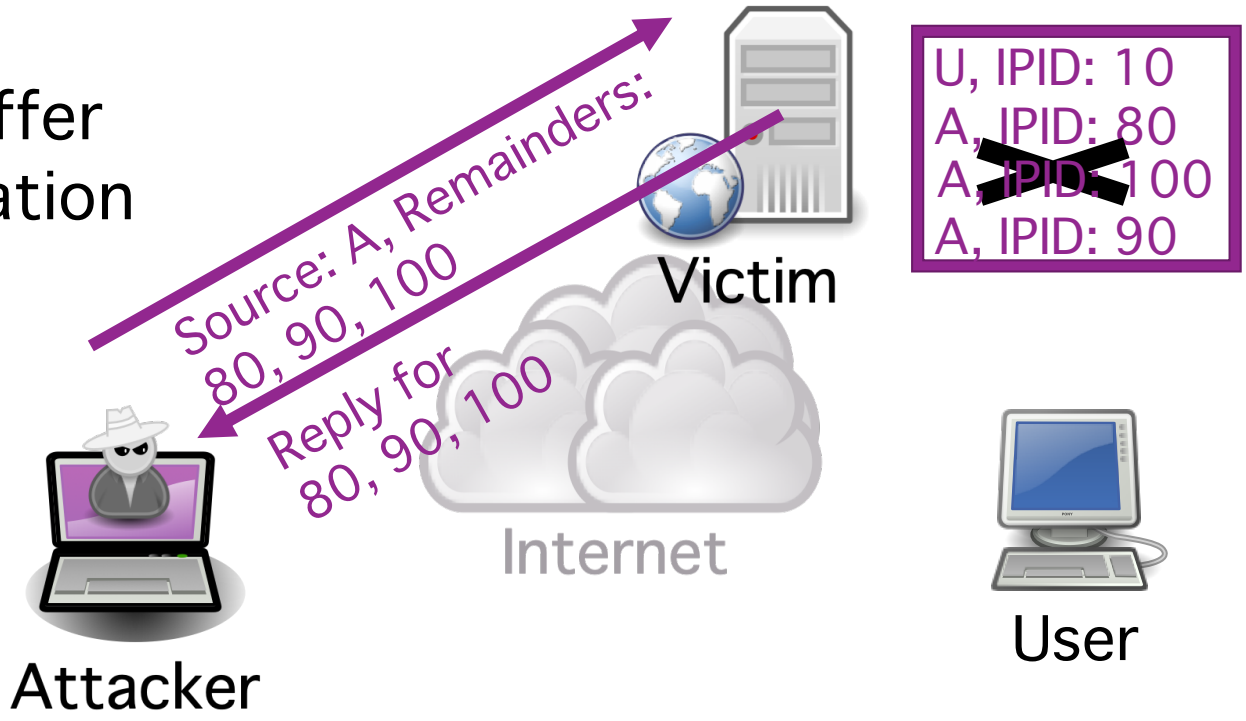
Buffer Side Channel

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



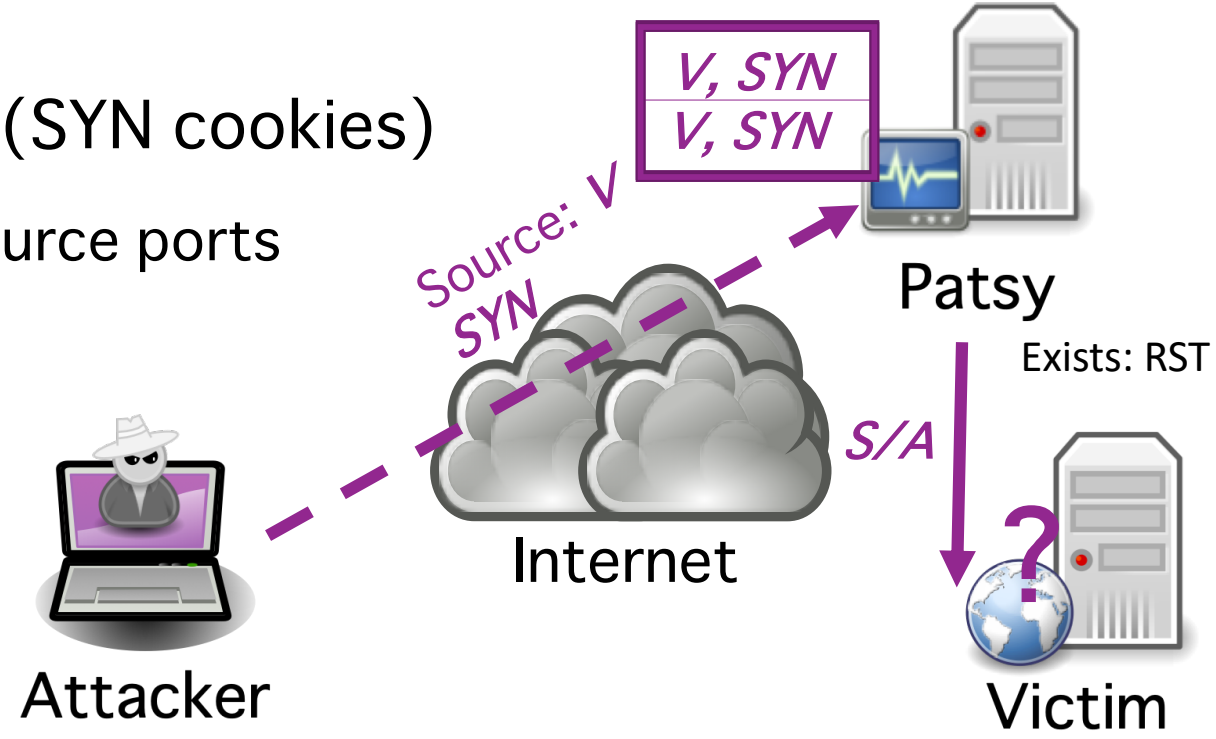
Buffer Side Channel

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



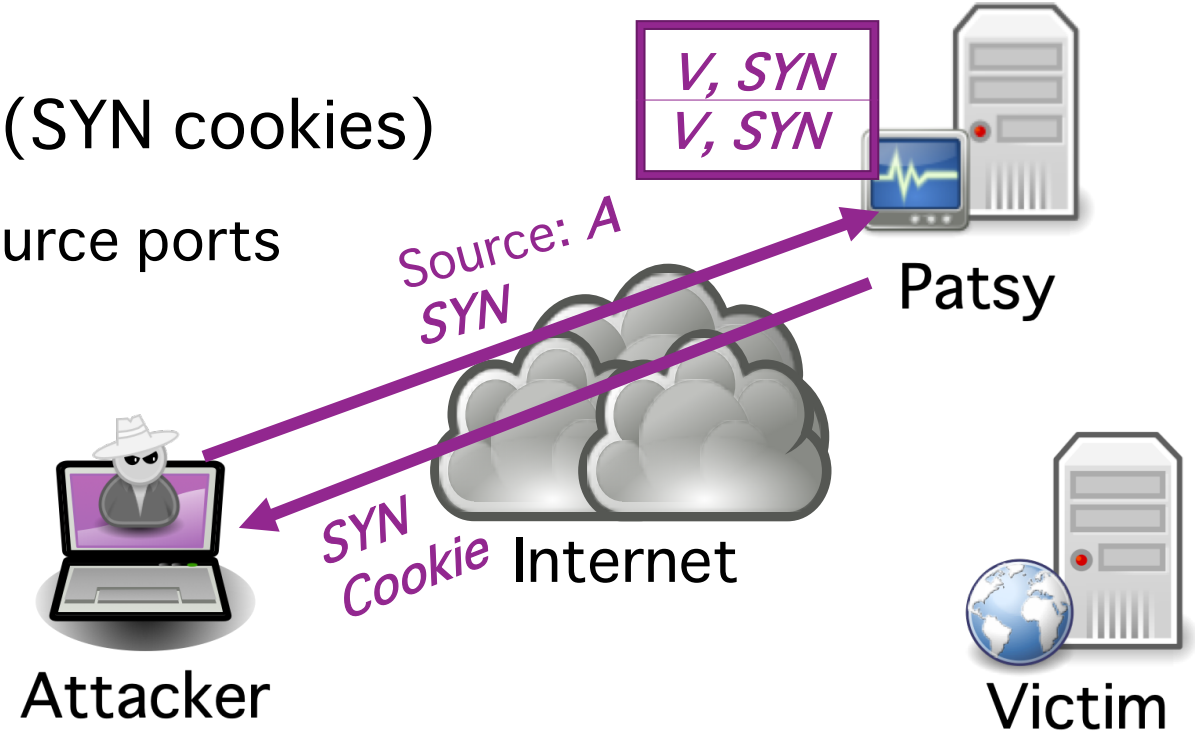
SYN Cache Side Channel

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



SYN Cache Side Channel

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



How to leverage?

- IPID:
  - Global --> straight forward
  - Per-Dest/2048 --> impossible/hard
- Timestamps --> straight forward
- Shared State --> overwhelm and check

My contributions

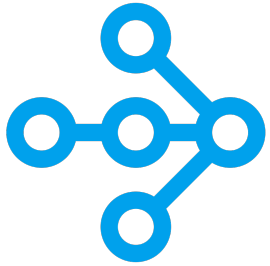
- Check for side-channel presence
  - Alexa Top 1000

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)

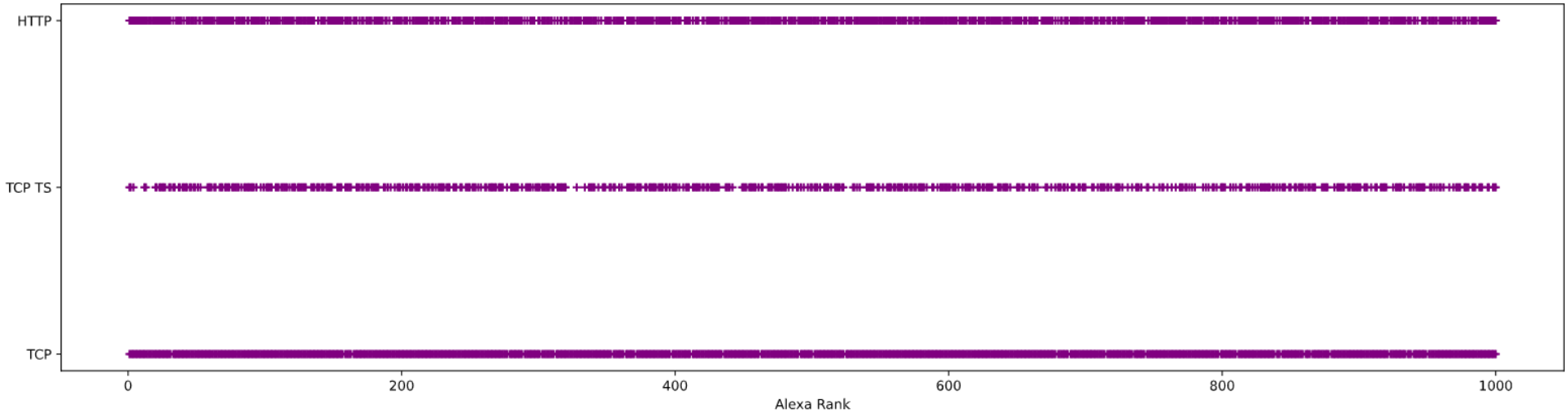


RAY

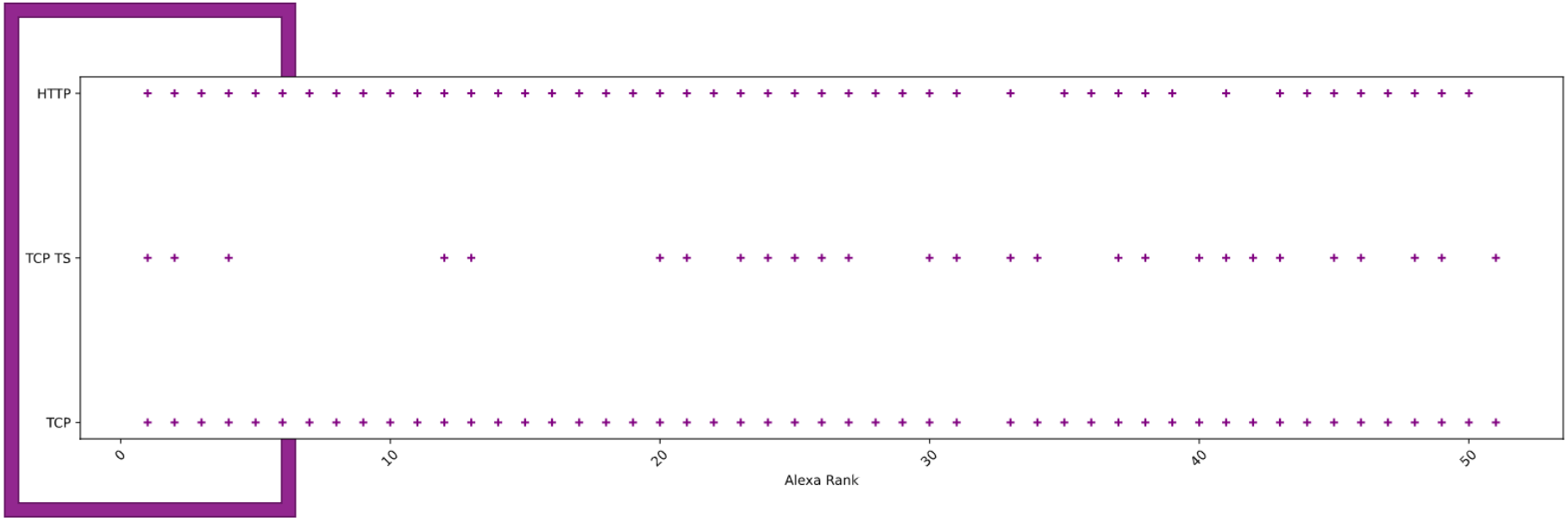
Results (a few)

- 986 responses
  - 98% had TCP responses
    - 60% had TCP timestamps
  - 85% had HTTP responses
  - 0 ICMP

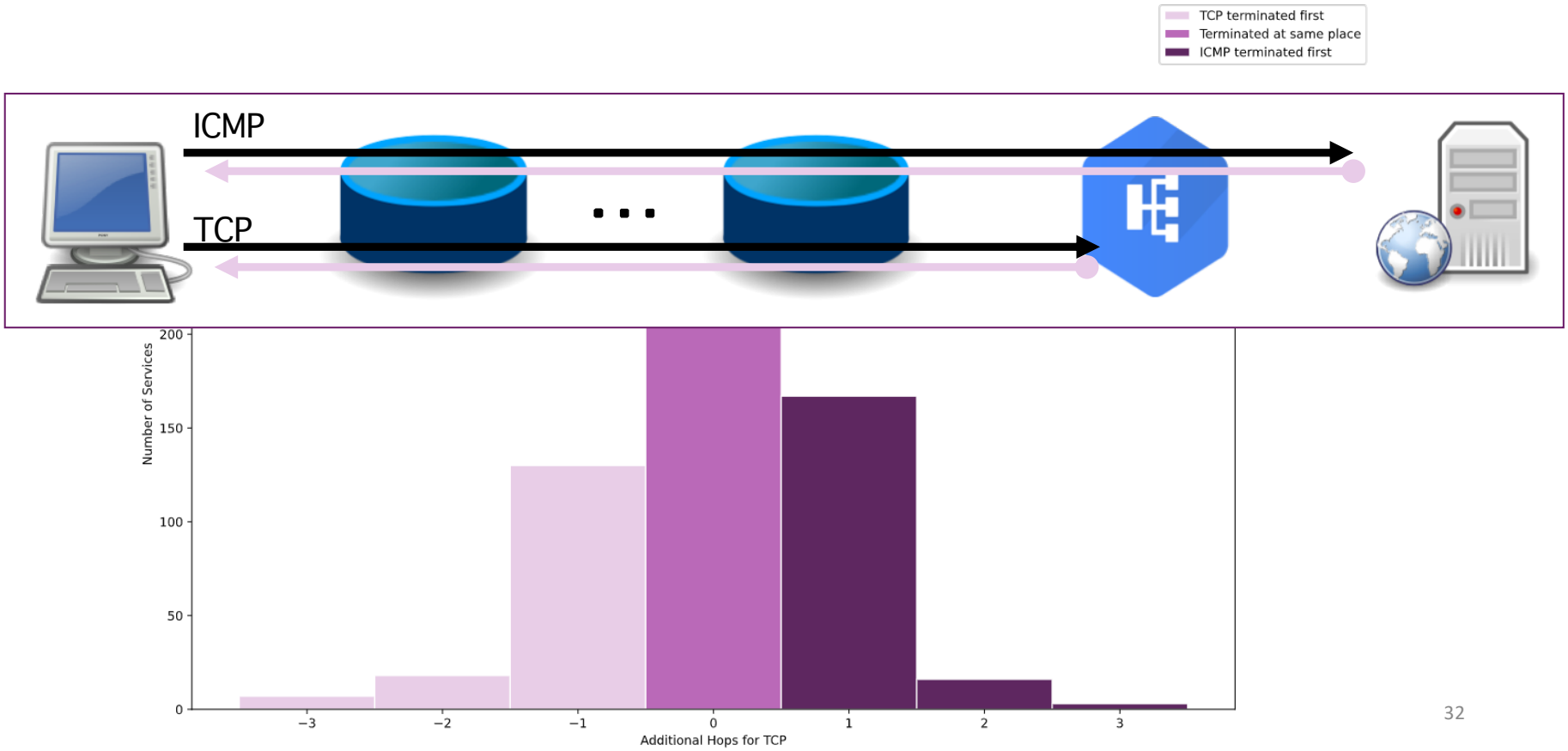
Results (a few)



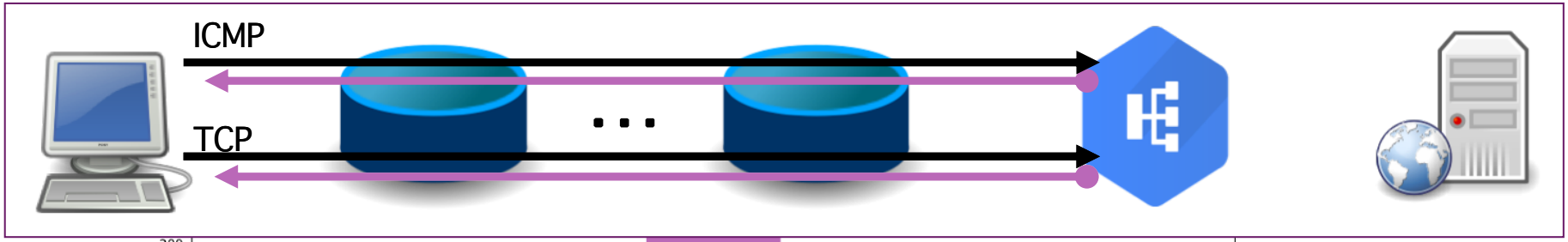
Results (a few)

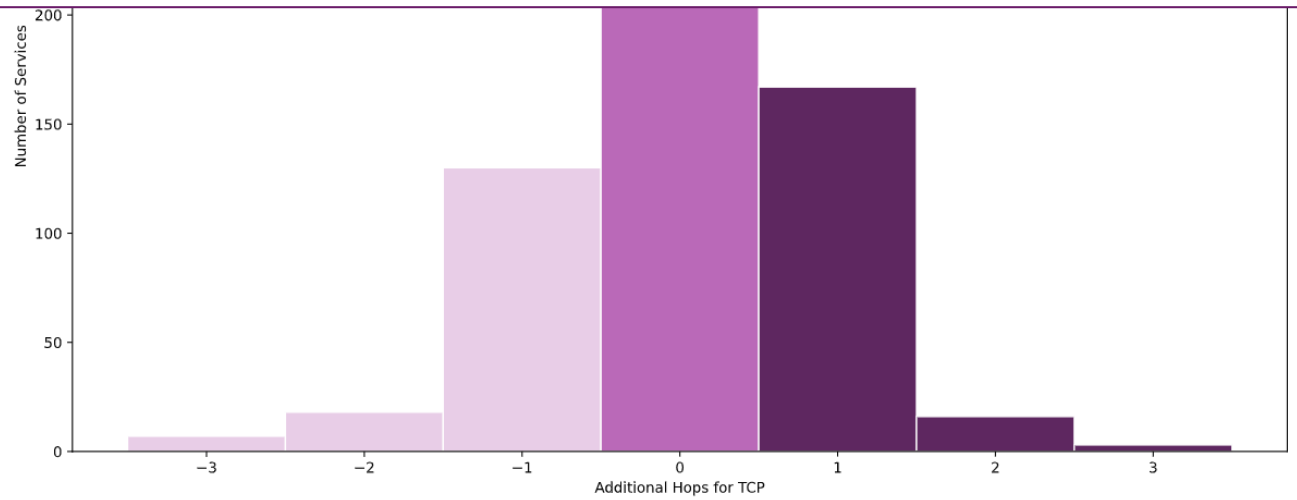


Results (a few)

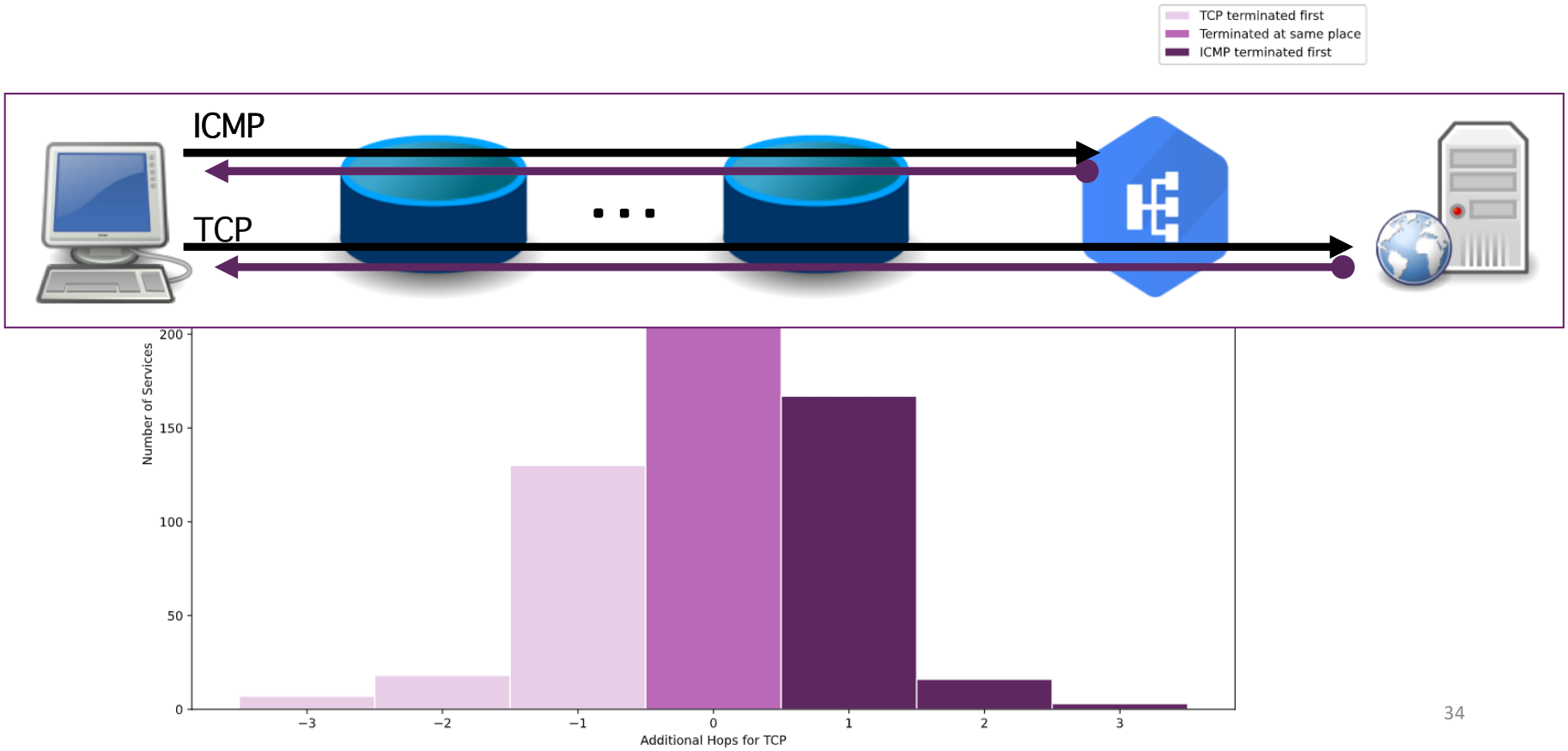


Results (a few)

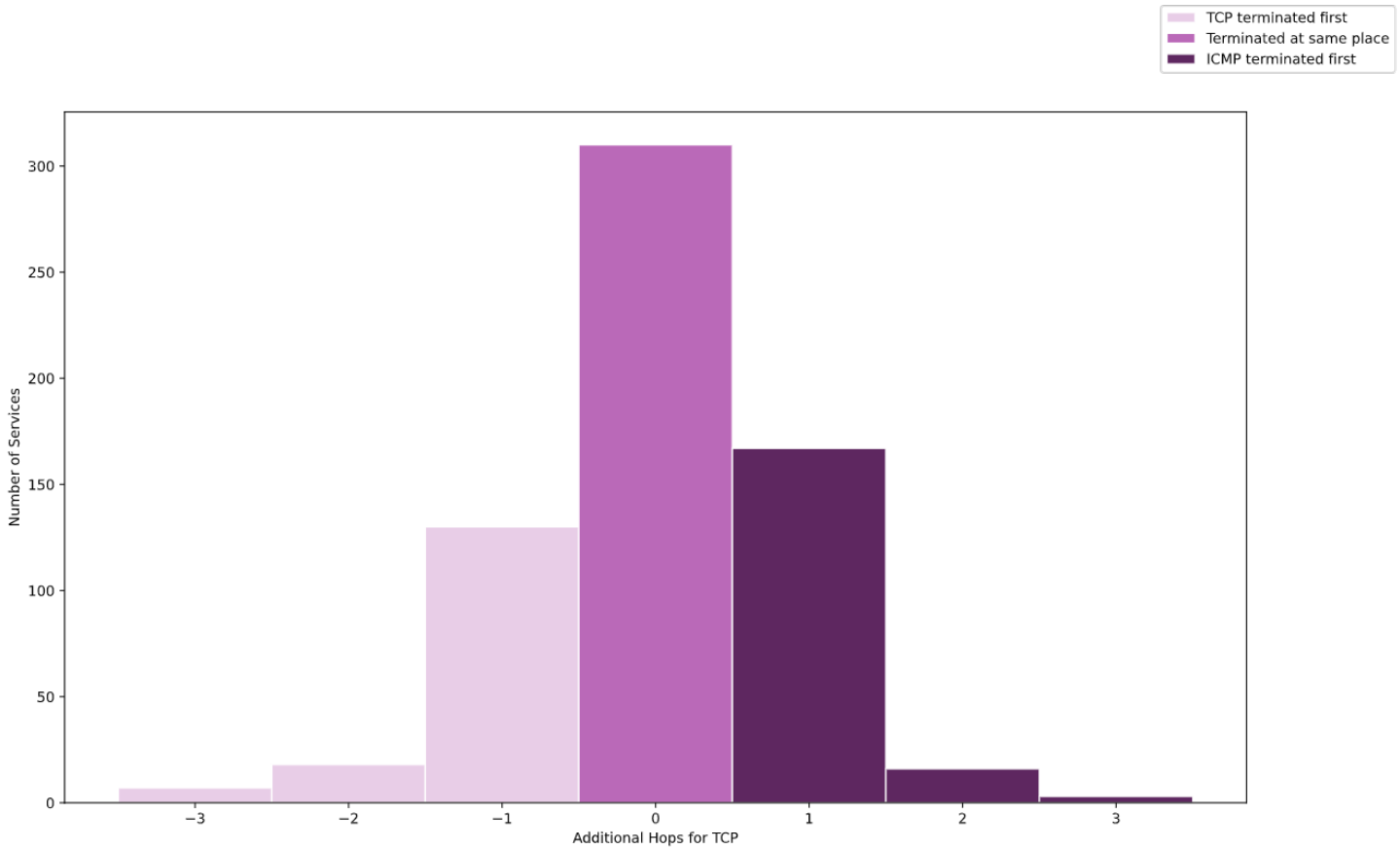




Results (a few)



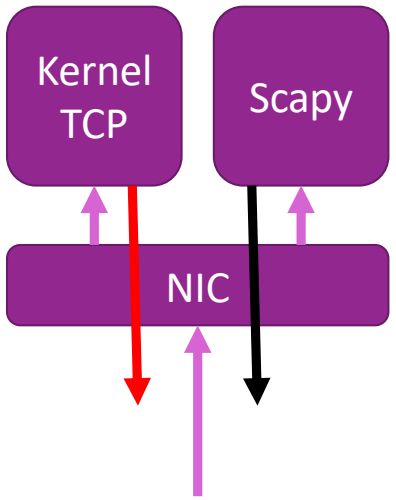
Results (a few)



Lessons Learned

- Don't underestimate the kernel

1.065417	192.168.42.20	172.217.164.1…	TCP	54	11339 → 80 [SYN] Seq=0 Win=8192 Len=0
1.069850	172.217.164.101	192.168.42.20	TCP	58	80 → 11339 [SYN, ACK] Seq=0 Ack=1 Win=60720 Len=0 MSS=1380
1.069894	192.168.42.20	172.217.164.1…	TCP	54	11339 → 80 [RST] Seq=1 Win=0 Len=0
1.078249	192.168.42.20	172.217.164.1…	TCP	54	11339 → 80 [ACK] Seq=1 Ack=1 Win=8192 Len=0
1.083304	172.217.164.101	192.168.42.20	TCP	54	80 → 11339 [RST] Seq=1 Win=0 Len=0



Lessons Learned

- Don't underestimate the kernel
- ISPs can be annoying

COX

ThisNameDoesNotExist.com cannot be found

Displaying search results for **ThisNameDoesNotExist.com**

Lessons Learned

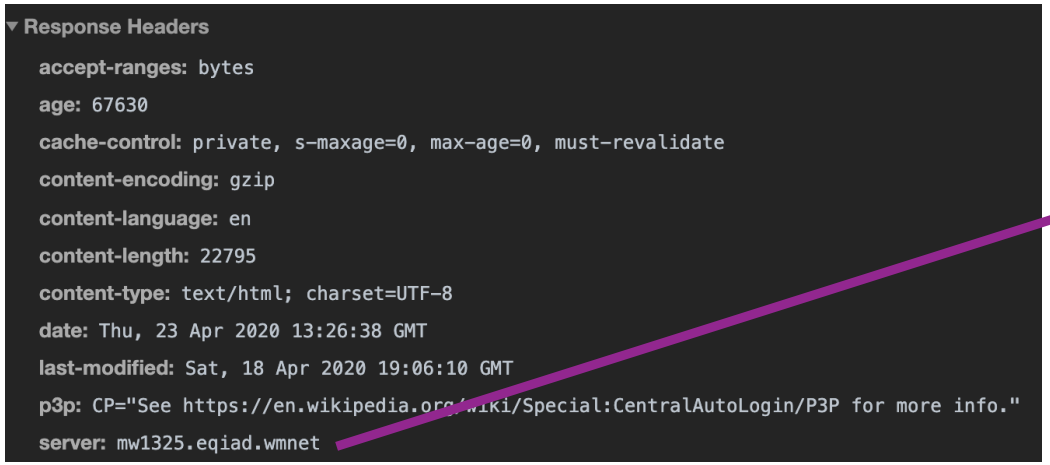
- Don't underestimate the kernel
- ISPs can be annoying
- I don't get IPv6
  - Google IPv6 DNS + IPv6 ISP support = No connection?!

Experiments Next Steps

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

Validation Next Steps

- Simple GCP Load Balanced Web Server
  - Easy ground-truth
- In-the-wild validation



Questions?

Thanks for listening!