

# CS165 – Computer Security

Network security 2

Nov 23, 2021

# Common network security attacks and their countermeasures

- Packet sniffing and spoofing
  - Encryption (SSH, SSL, HTTPS)
- Finding a way into the network
  - Firewalls
- Exploiting software bugs, buffer overflows
  - Intrusion Detection Systems
- Denial of Service
  - Ingress filtering, IDS



# Finding a way into the network -- Scanning

Host 192.168.2.1 appears to be up.

MAC Address: 00:04:E2:34:B6:CE (SMC Networks)

Host 192.168.2.79 appears to be up.

MAC Address: 00:11:11:5B:7A:CD (Intel)

Host 192.168.2.82 appears to be up.

MAC Address: 00:10:5A:0D:F6:D7 (3com)

Host 192.168.2.198 appears to be up.

MAC Address: 00:10:DC:55:89:27 (Micro-star International)

Host 192.168.2.199 appears to be up.

MAC Address: 00:C0:4F:36:33:91 (Dell Computer)

Host 192.168.2.200 appears to be up.

MAC Address: 00:0C:41:22:CC:01 (The Linksys Group)

Host 192.168.2.251 appears to be up.

MAC Address: 00:0F:66:75:3D:75 (Cisco-Linksys)

# Does That Matter?

- The number of computers an organization has roughly corresponds to the number of people in it
- How large is your competitor?
- (How many computers does Google have in its data centers? They won't say.)

# Does That Matter?

- If they identify a service that has a known vulnerability (e.g., buffer overflow), they can launch the corresponding exploit

```
$ nmap -Pn www.cs.ucr.edu
```

```
Starting Nmap 6.40 ( http://nmap.org ) at 2015-11-17 20:03 UTC
```

```
Nmap scan report for www.cs.ucr.edu  
(169.235.30.15)
```

```
Host is up (0.00033s latency).
```

```
rDNS record for 169.235.30.15: thoth.cs.ucr.edu
```

```
Not shown: 996 closed ports
```

```
PORT      STATE SERVICE
```

```
22/tcp    open  ssh
```

```
80/tcp    open  http
```

```
111/tcp   open  rpcbind
```

```
5666/tcp  open  nrpe
```

# Firewalls



- Basic problem – many network applications and protocols have security problems that are fixed over time
  - Difficult for users to keep up with changes and keep host secure
  - Solution
    - Administrators limit access to end hosts by using a firewall
    - Firewall is kept up-to-date by administrators

# Firewalls



- A firewall is like a castle with a drawbridge
  - Only one point of access into the network
  - This can be good or bad
- Can be hardware or software
  - Ex. Some routers come with firewall functionality
  - ipfw, ipchains, pf on Unix systems, Windows XP and Mac OS X have built in firewalls

# Firewalls



- Used to filter packets based on a combination of features
  - These are called packet filtering firewalls
    - There are other types too, but they will not be discussed
  - Ex. Drop packets with destination port of 23 (Telnet)
  - Can use any combination of IP/UDP/TCP header information
- But why don't we just turn Telnet off?



# Firewalls



- Here is what a computer with a default Windows install looks like:

- 135/tcp open loc-srv
- 139/tcp open netbios-ssn
- 445/tcp open microsoft-ds
- 1025/tcp open NFS-or-IIS
- 3389/tcp open ms-term-serv
- 5000/tcp open UPnP

# Common network security attacks and their countermeasures

- Packet sniffing and spoofing
  - Encryption (SSH, SSL, HTTPS)
- Finding a way into the network
  - Firewalls
- Exploiting software bugs, buffer overflows
  - Intrusion Detection Systems
- Denial of Service
  - Ingress filtering, IDS



# Intrusion Detection



- Used to monitor for “suspicious activity” on a network
  - Can protect against known software exploits, like buffer overflows
- Open Source IDS:
  - Snort, [www.snort.org](http://www.snort.org)
  - Bro
- Monitor payload of packets
  - Modern firewalls also do that (blurred definition)

# Intrusion Detection



- Uses “intrusion signatures”
  - Well known patterns of behavior
    - Ping sweeps, port scanning, web server indexing, OS fingerprinting, DoS attempts, etc.
- Example
  - IRIX vulnerability in `webdist.cgi`
  - Can make a rule to drop packets containing the line
    - `“/cgi-bin/webdist.cgi?distloc=?;cat%20/etc/passwd”`
- However, IDS is only useful against certain forms of attacks
  - What if traffic is encrypted?
  - What if an attacker can morph into a different payload?

# Common network security attacks and their countermeasures

- Packet sniffing and spoofing
  - Encryption (SSH, SSL, HTTPS)
- Finding a way into the network
  - Firewalls
- Exploiting software bugs, buffer overflows
  - Intrusion Detection Systems
- Denial of Service
  - Ingress filtering, IDS

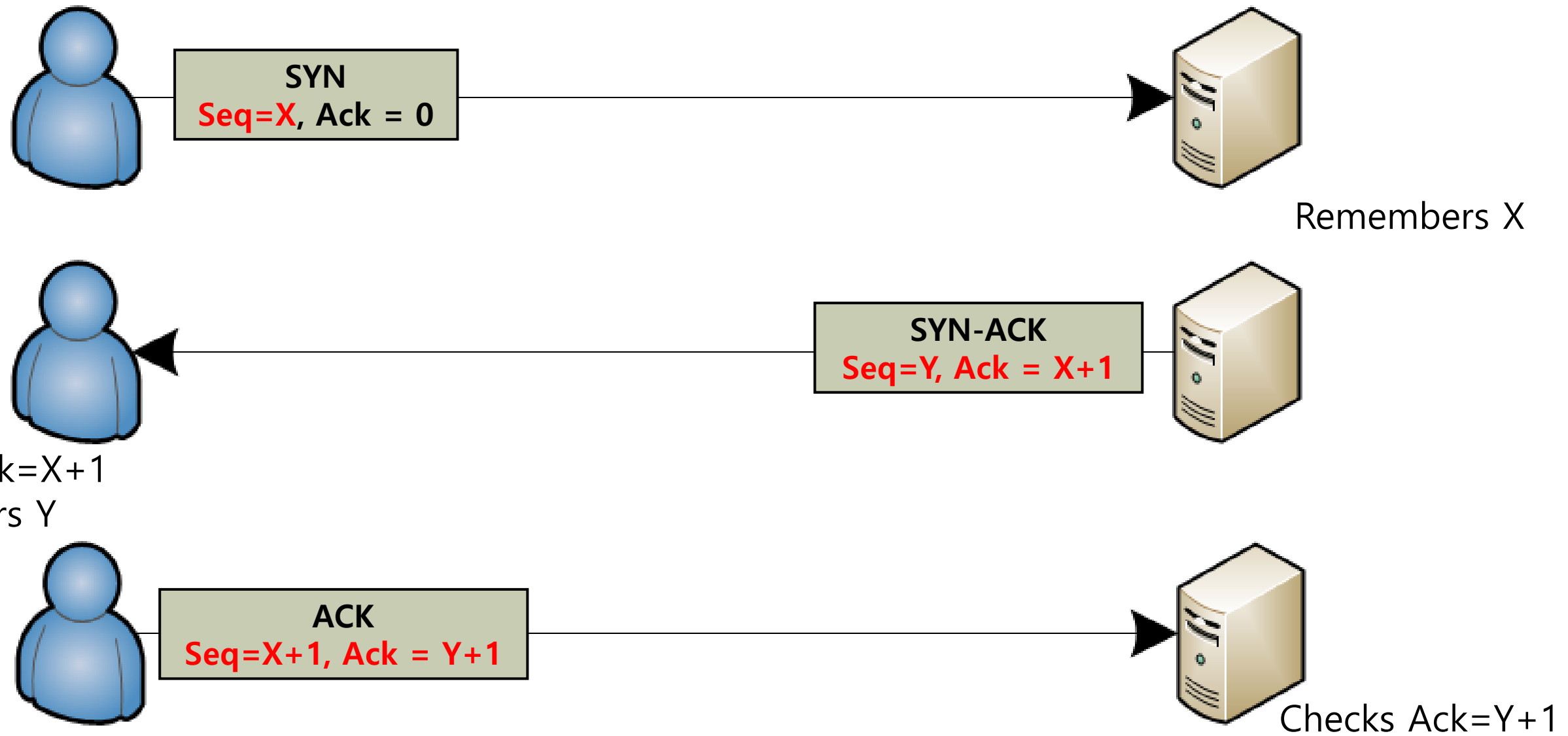


# Denial of Service

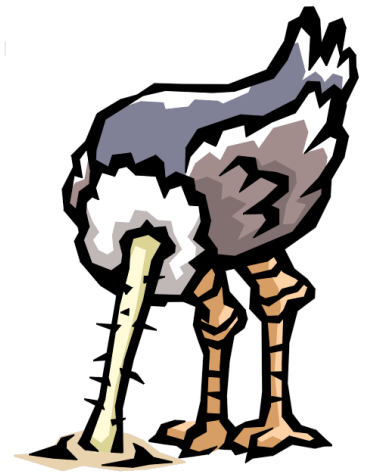


- Purpose: Make a network service unusable, usually by overloading the **server or network**
- General strategies of DoS attacks
  - Attacker: small resource -> amplifying impact
  - Attacker: large resource -> bruteforce

# TCP Three-way handshake



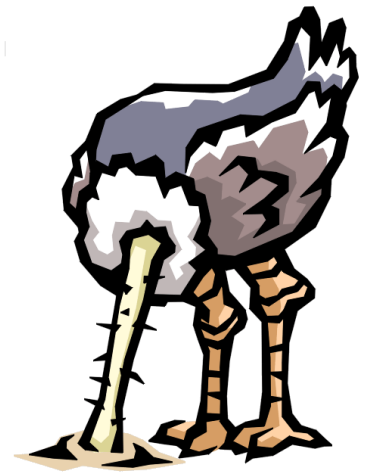
# Denial of Service



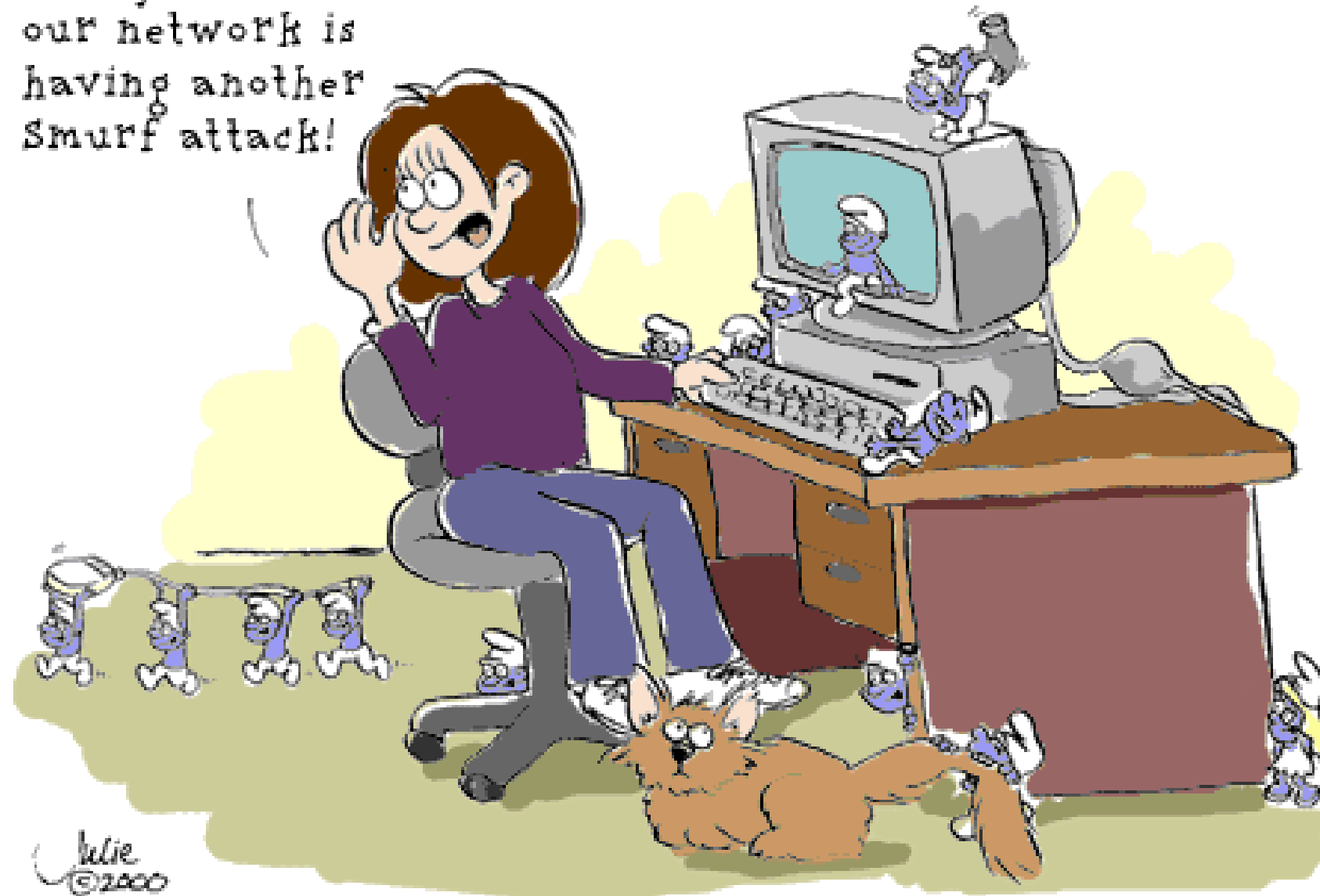
- SYN flooding attack
- Send SYN packets with spoofed/bogus source address
  - Why?
- Server responds with SYN ACK and keeps state about TCP half-open connection
  - Eventually, server memory is exhausted with this state



# Denial of Service



Honey! I think  
our network is  
having another  
Smurf attack!



# Denial of Service

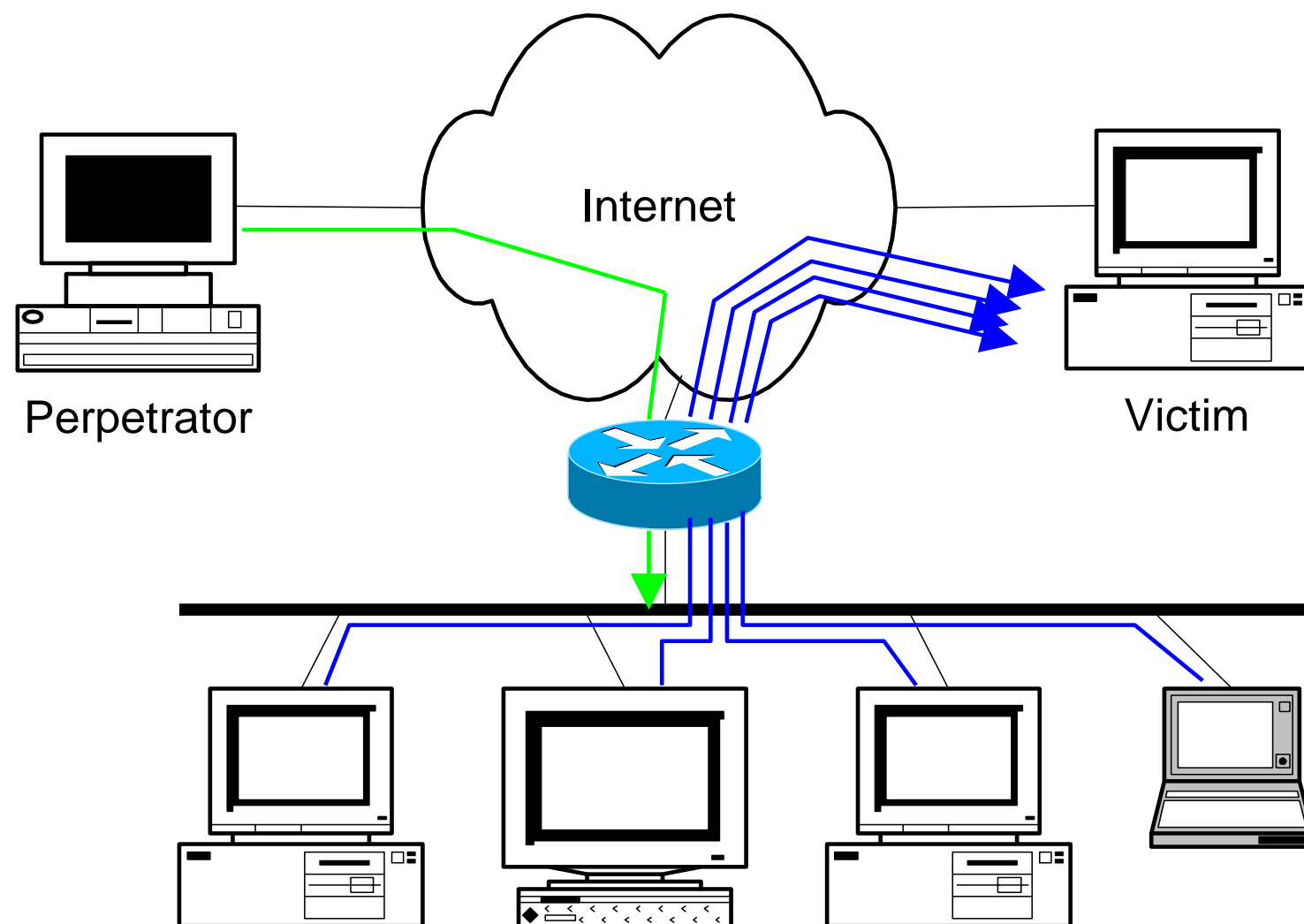


- SMURF
  - Source IP address of a broadcast ping is forged
  - Large number of machines respond back to victim, overloading it

# Denial of Service

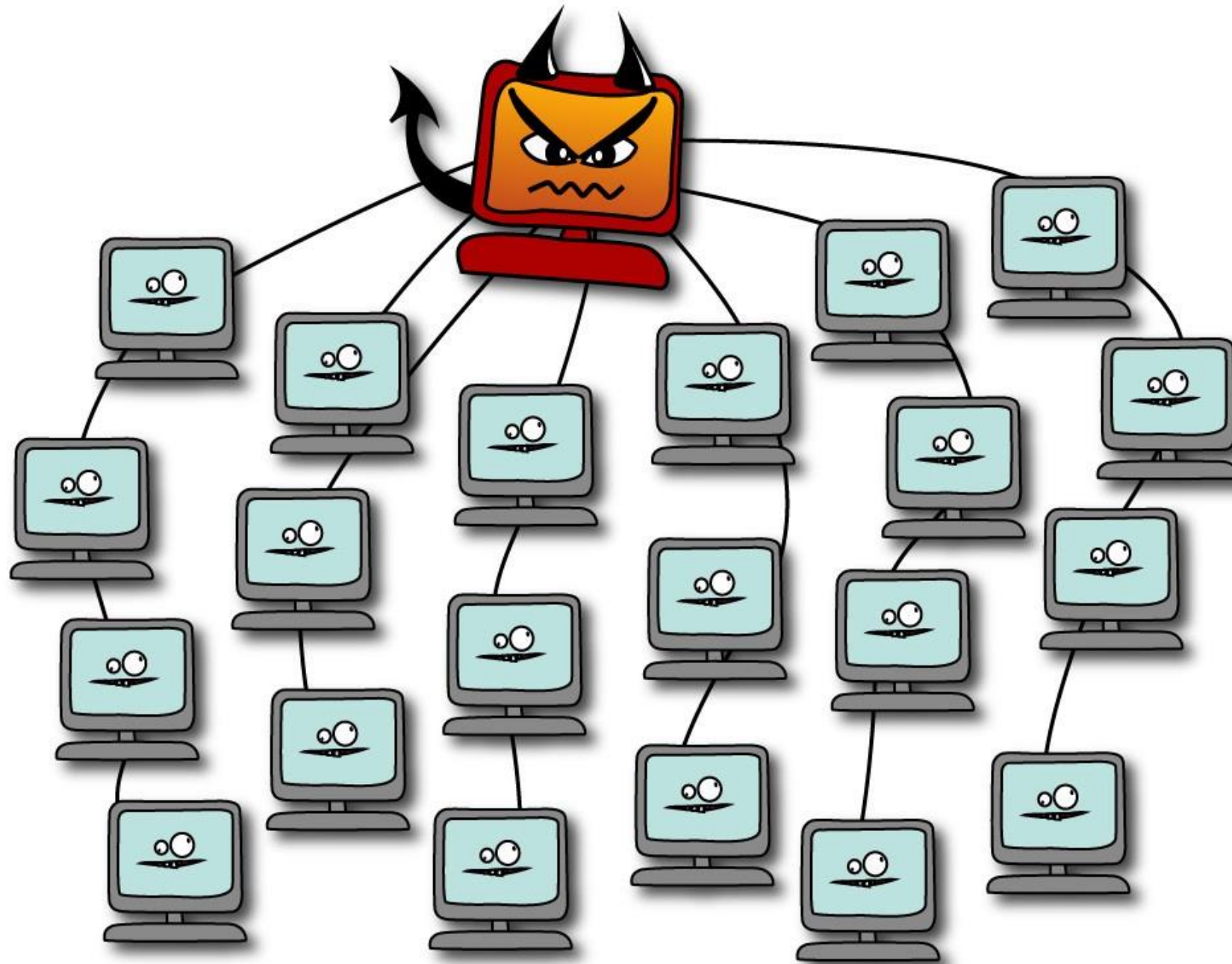


- ICMP echo (spoofed source address of victim)  
Sent to IP broadcast address
- ICMP echo reply



# Denial of Service

- Distributed attacks, e.g., botnet

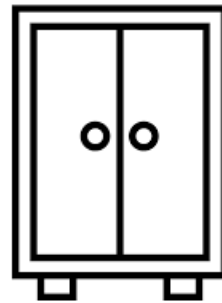


# Common network security attacks and their countermeasures

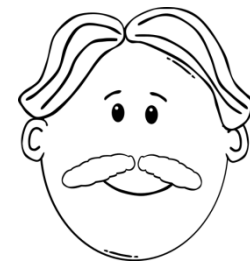
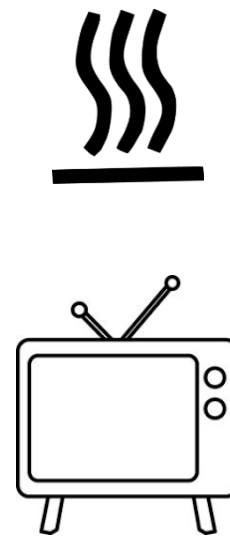
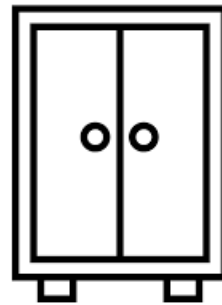
- Packet sniffing and spoofing
  - Encryption (SSH, SSL, HTTPS)
- Finding a way into the network
  - Firewalls
- Exploiting software bugs, buffer overflows
  - Intrusion Detection Systems
- Denial of Service
  - Ingress filtering, IDS
- Advanced topic: network side channels



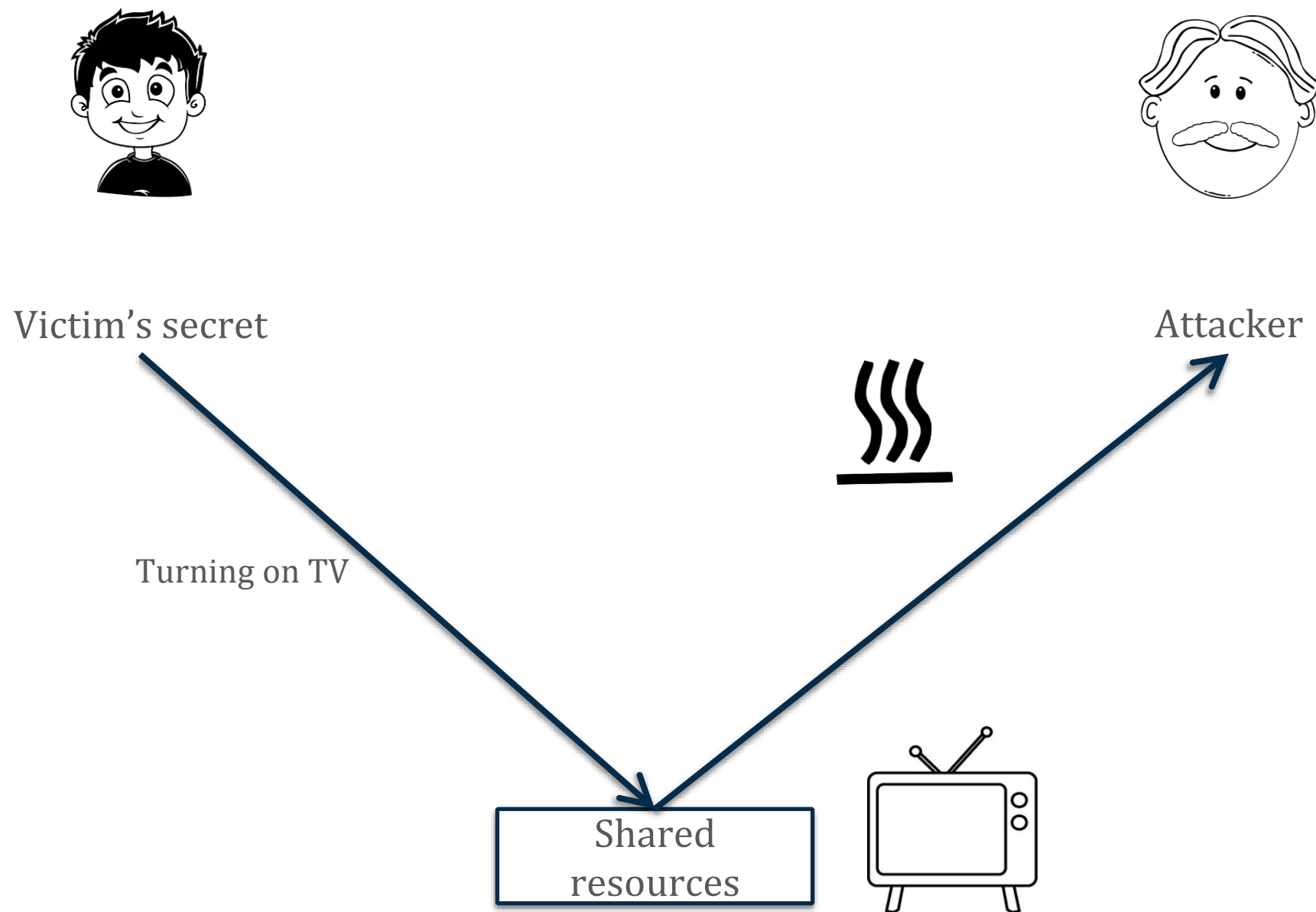
# Side Channel Example



# Side Channel Example



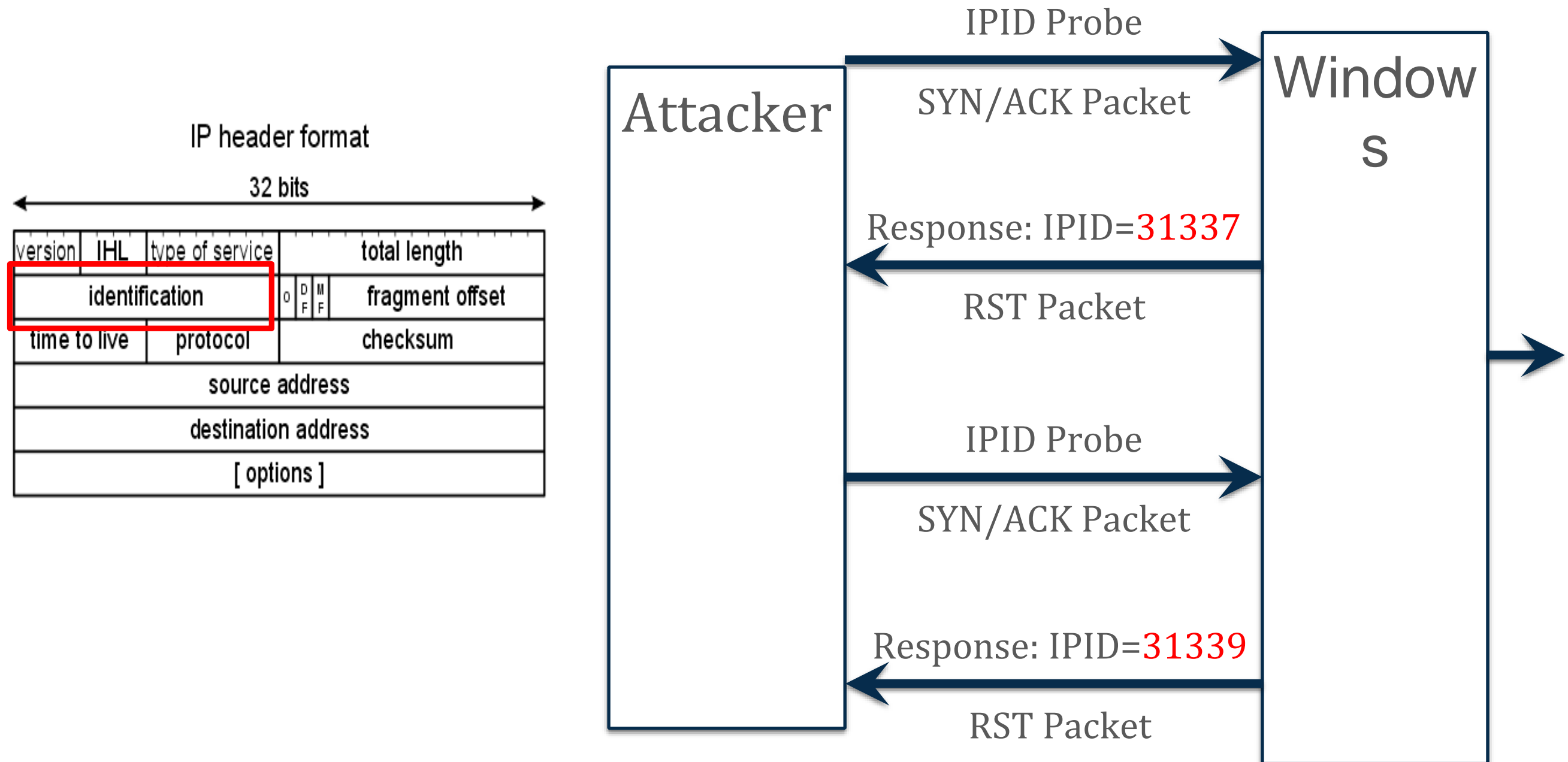
# Side Channel Example





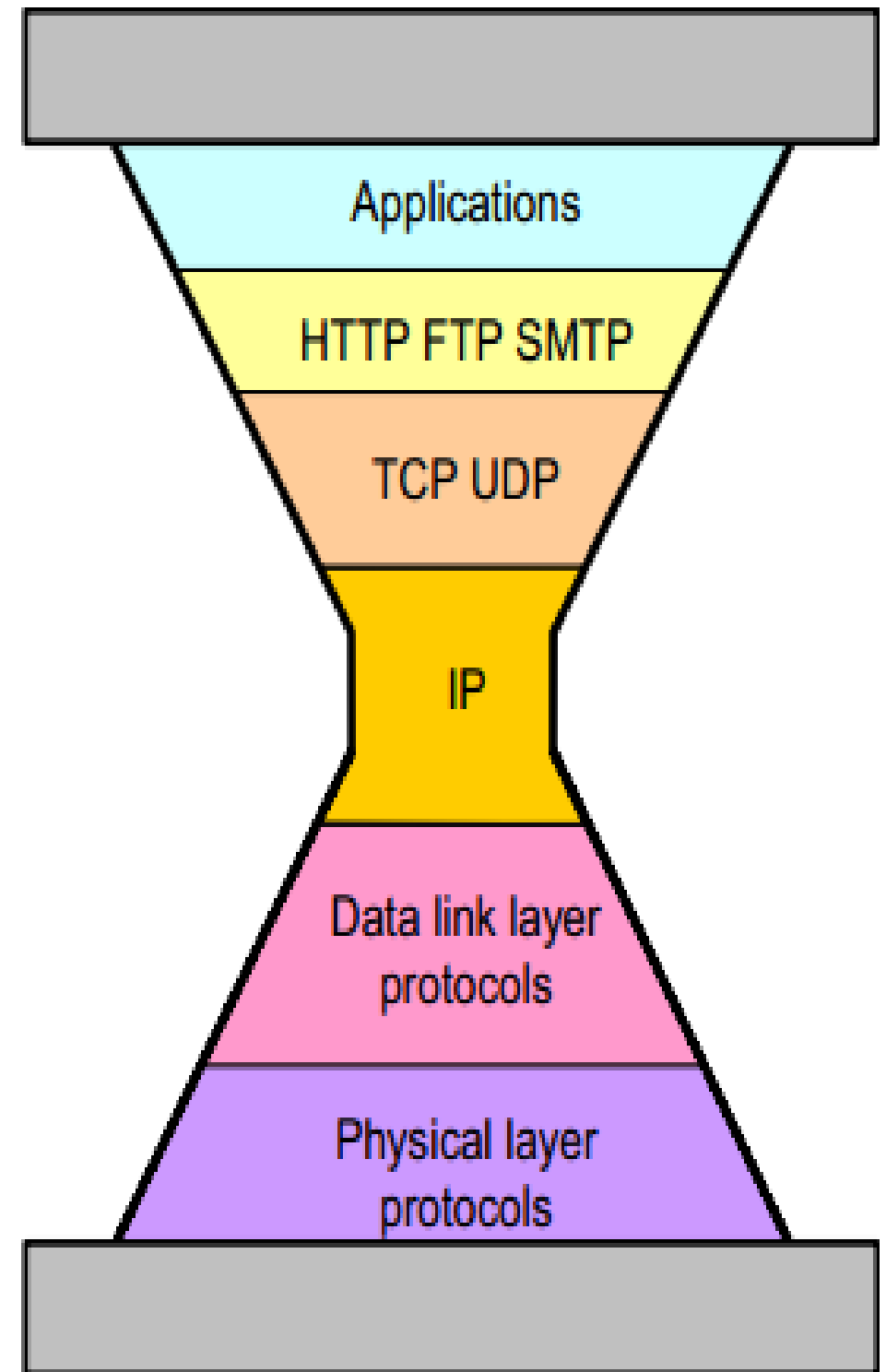
# Network Side Channels – a flashback (1999)

- Side channel: Incrementing IPIDs on Windows and other selected Oses



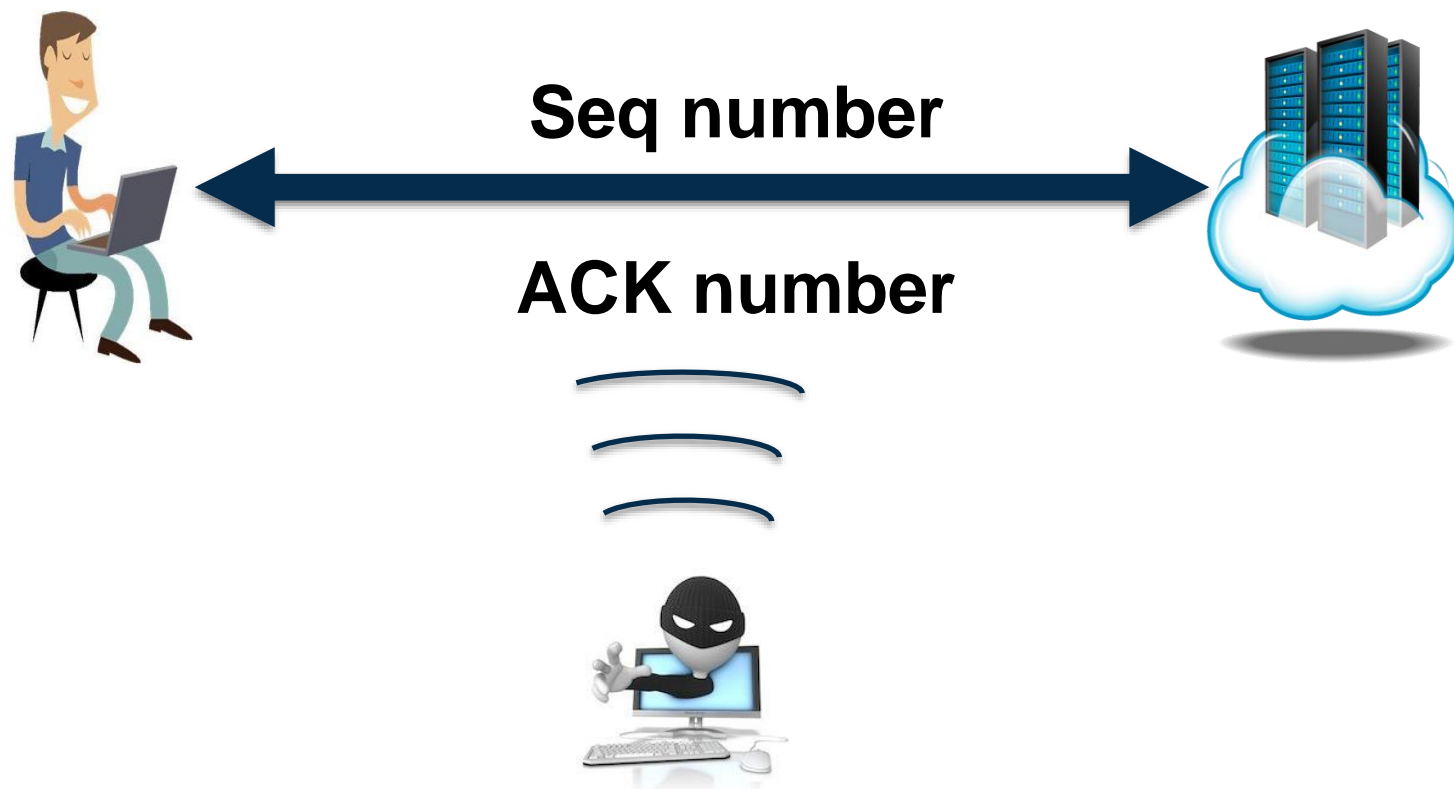
# TCP Side Channels

- Decades old and fundamental
- Unique position in the protocols
- Interact with other layers
- Holds important secrets



# Secrets in TCP




- Threat model: a blind off-path attacker
- Secrets:
  - Presence of a connection
  - Sequence number in both directions
- Assumption: Crafting IP-spoofed packets



# Off-path attack against TCP

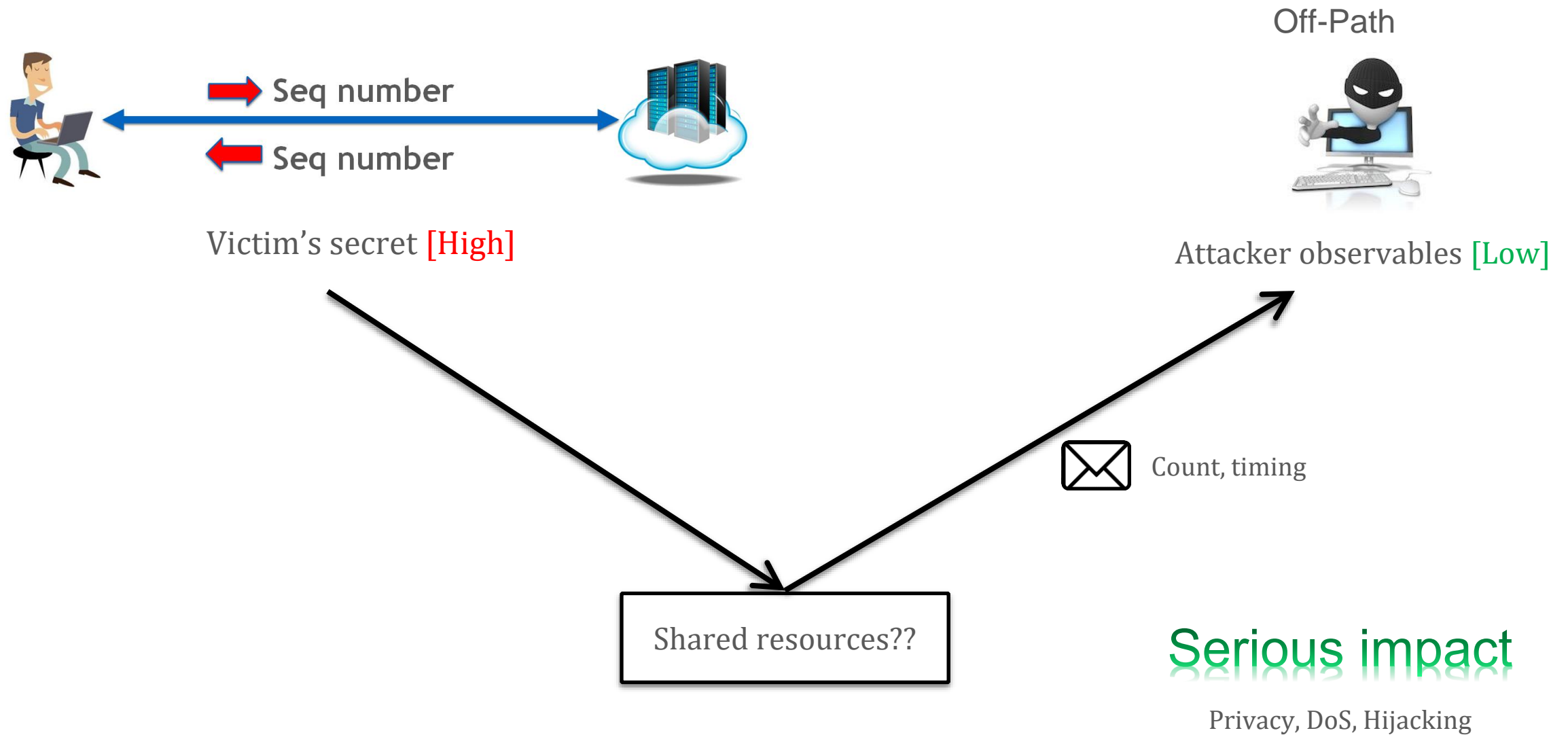
- Need to guess the **port number, sequence number, and acknowledgement number!**



 IP header  
 TCP header  
 Payload

What about eavesdropping and MITM?

# Shared Resources in TCP?



# DEMO: Malware-Assisted Attack [\[Oakland 2012, CCS 2012\]](#)

# Shared Resource: *Global* Rate Limit

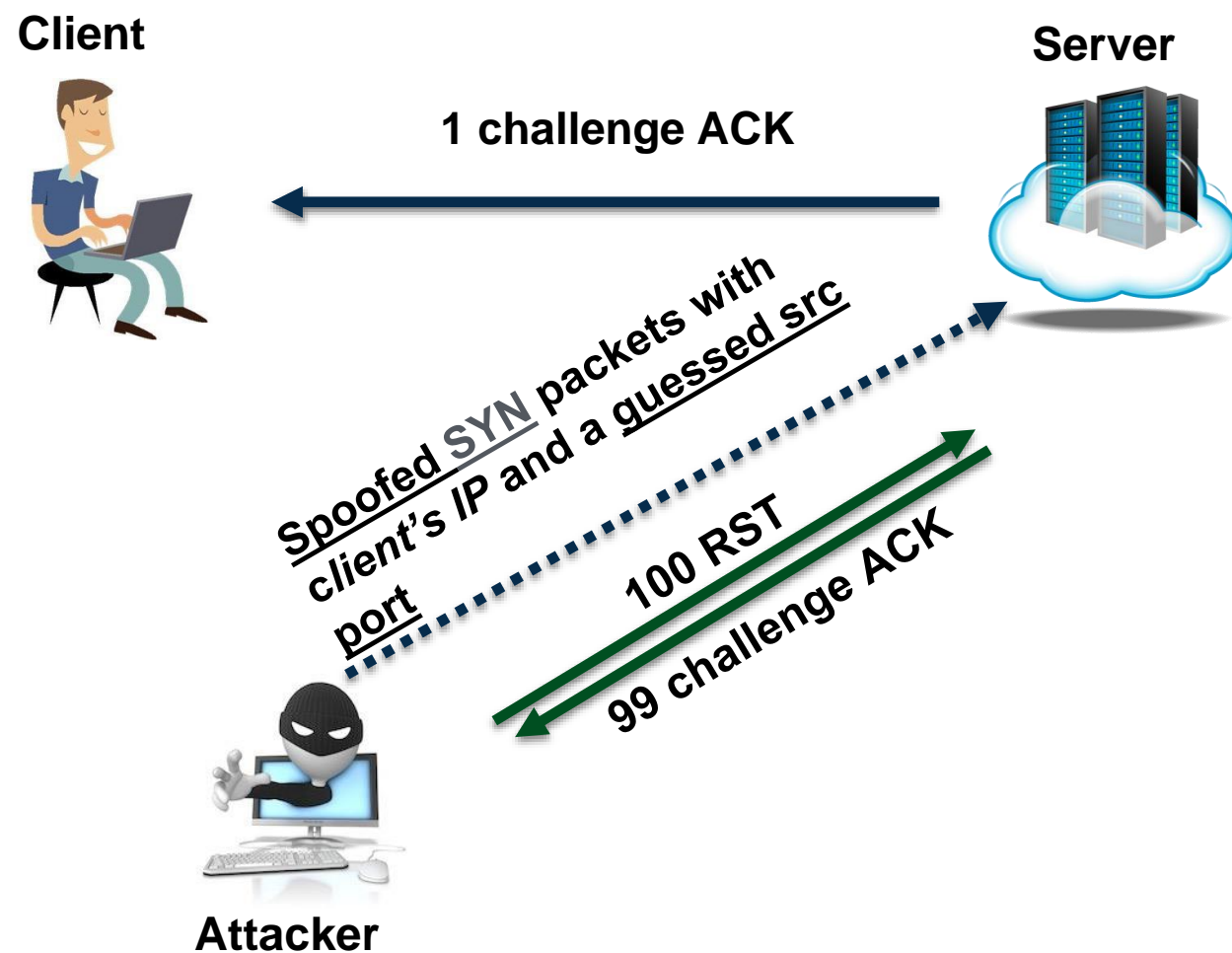
- Since Linux 3.6+
  - Challenge ACK rate limit **shared** across all connections
  - Default: 100 per second



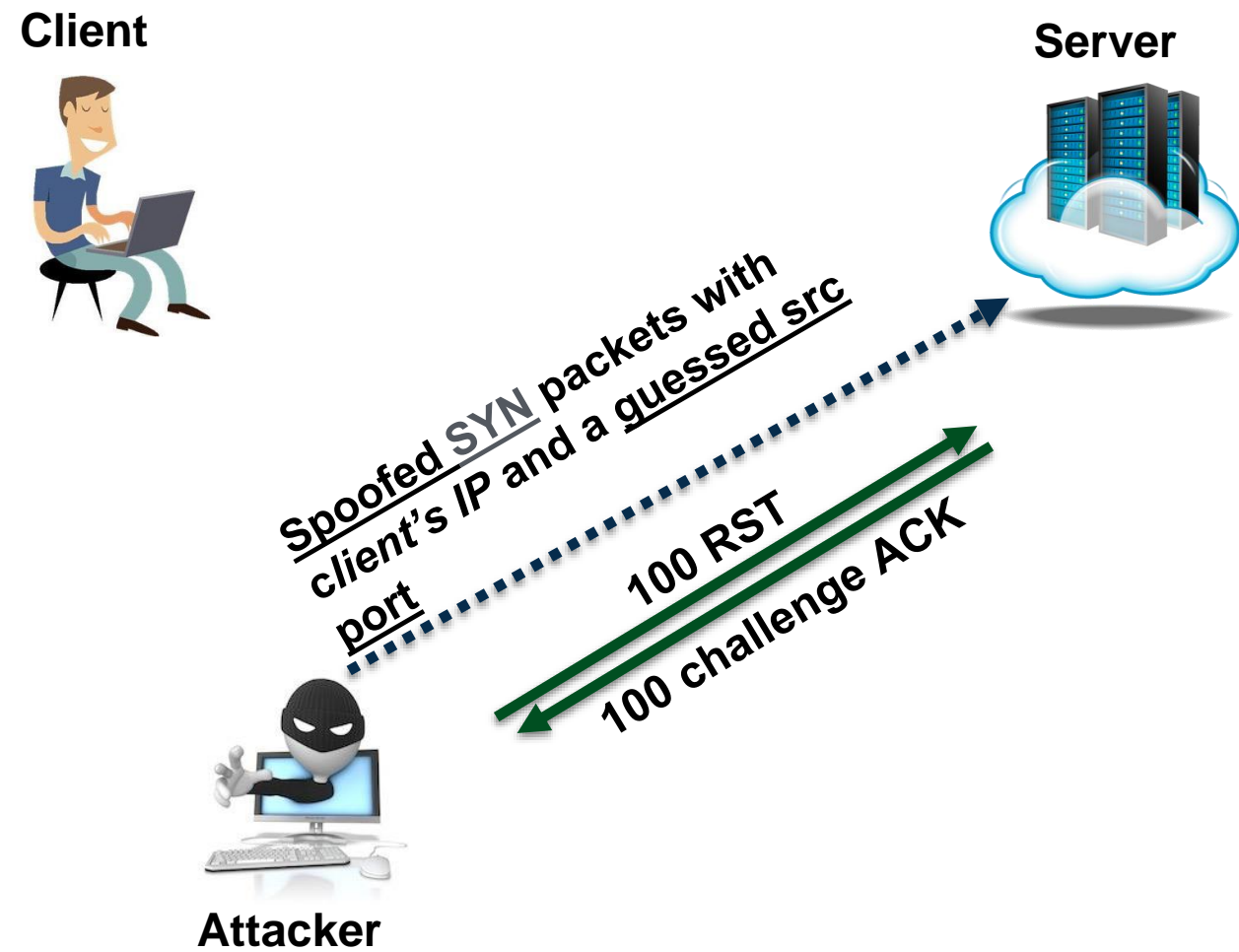
# Exploit the Vulnerability

– Example: to guess correct client port number

- If it's a correct guess:



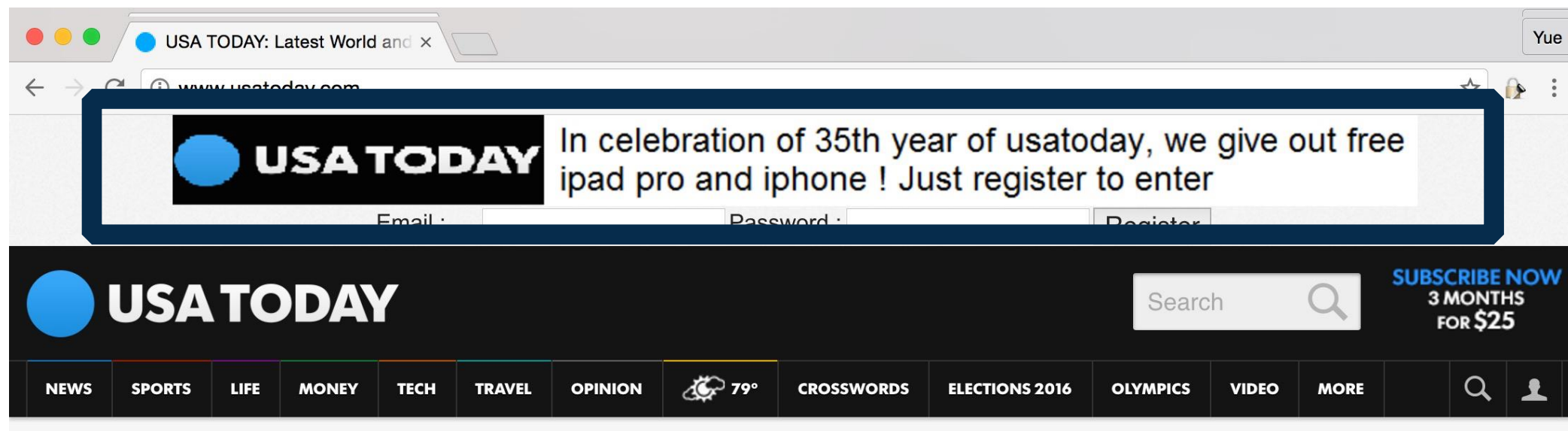
- If it's a wrong guess:





# Evaluation

- Existence of connection: <10 seconds
- Sequence number: 30 seconds
- ACK number: <10 seconds



# Lessons Learned

- Cannot ignore any small shared resources
- Reported to Linux

Patched and TCP specification (RFC 5961) amended

- Can we enumerate these shared resources? All in software.

## **Principled Unearthing of TCP Side Channel Vulnerabilities**

Yue Cao, Zhongjie Wang, Zhiyun Qian, Chengyu Song, Srikanth Krishnamurthy, Paul Yu

*In Proceedings of ACM Conference on Computer and Communications Security (CCS) 2019, London, UK.*

# **DNS Cache Poisoning Attack Reloaded: Revolutions with Side Channels**

ACM CCS 2020

Distinguished Paper Award

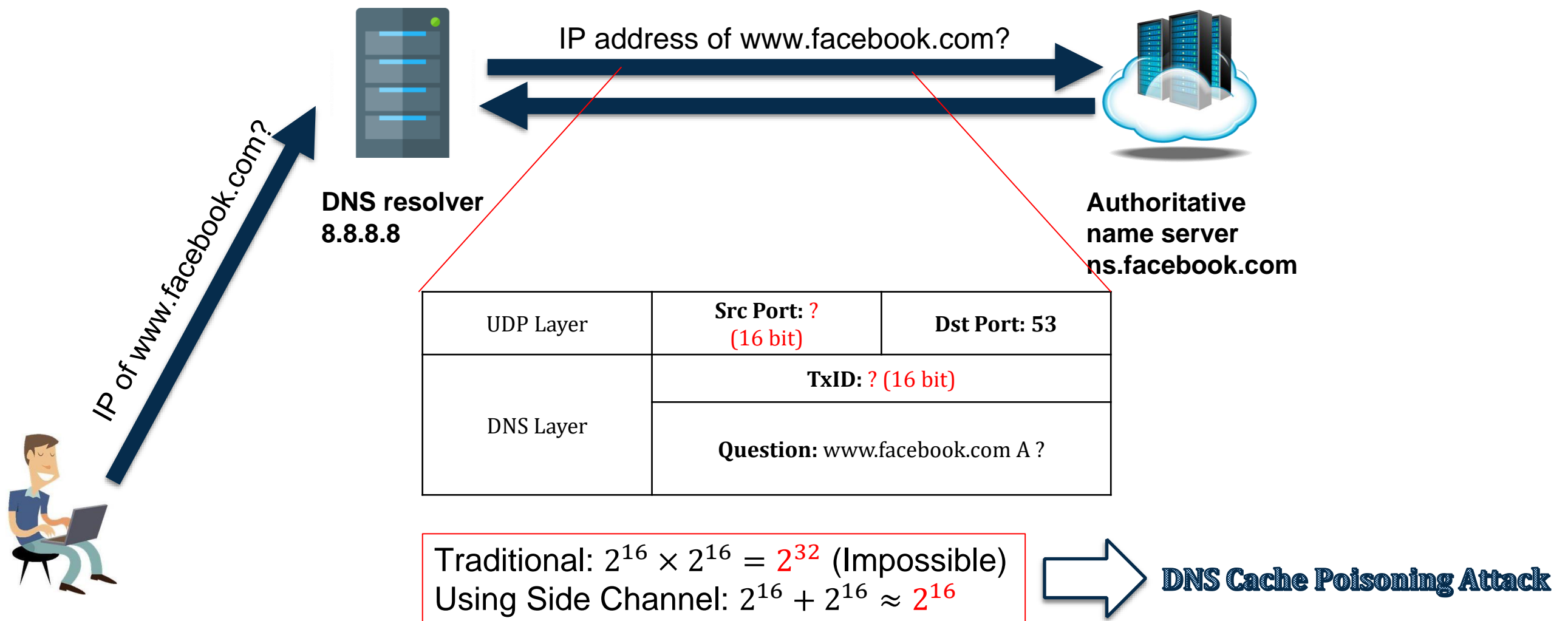
# Side Channels in UDP

- Secrets
  - Presence of a UDP session

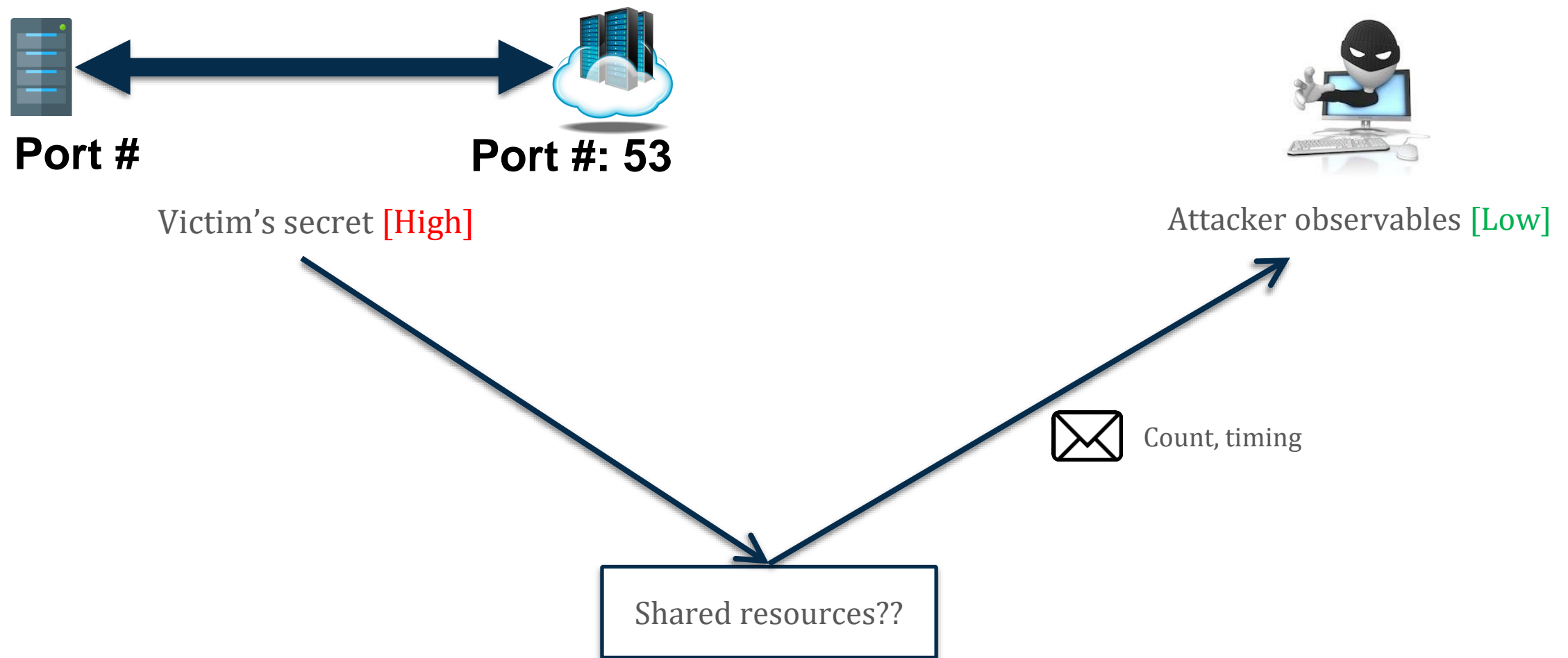


# Side Channels in UDP

- Security of DNS relies on
  - Randomized source port of DNS requests

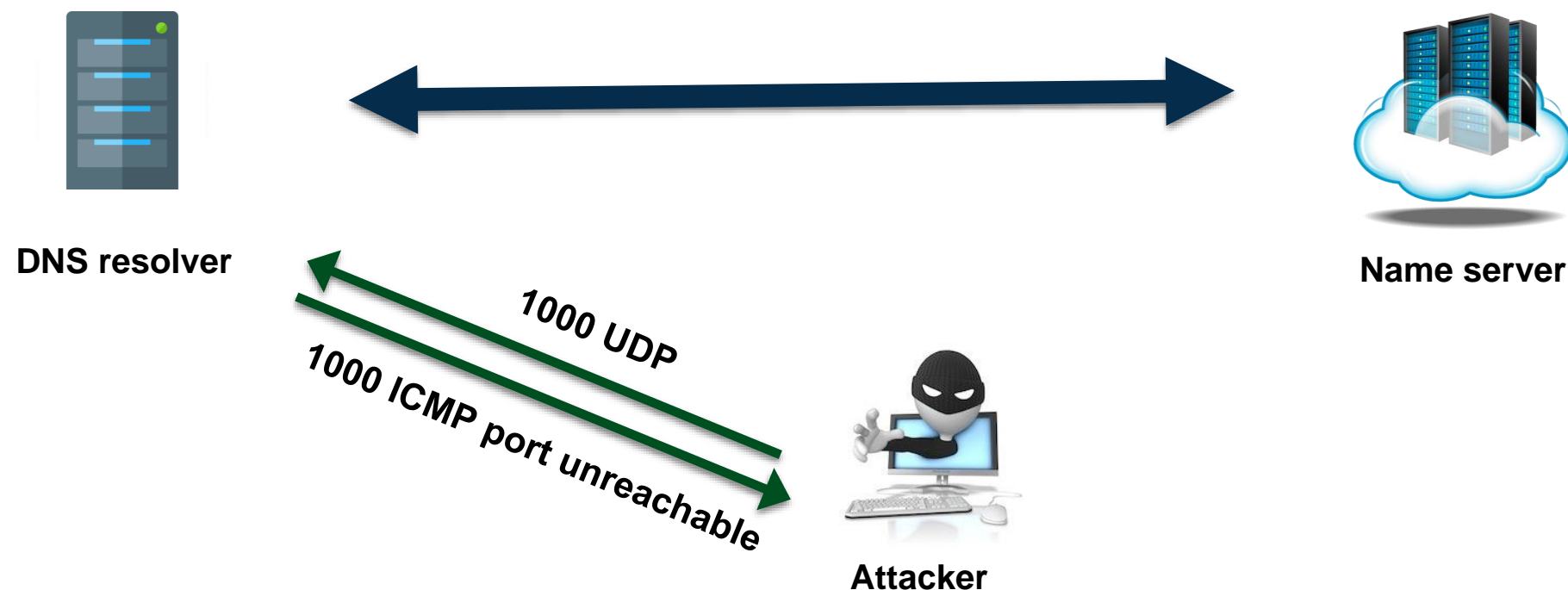


# Side Channels in UDP



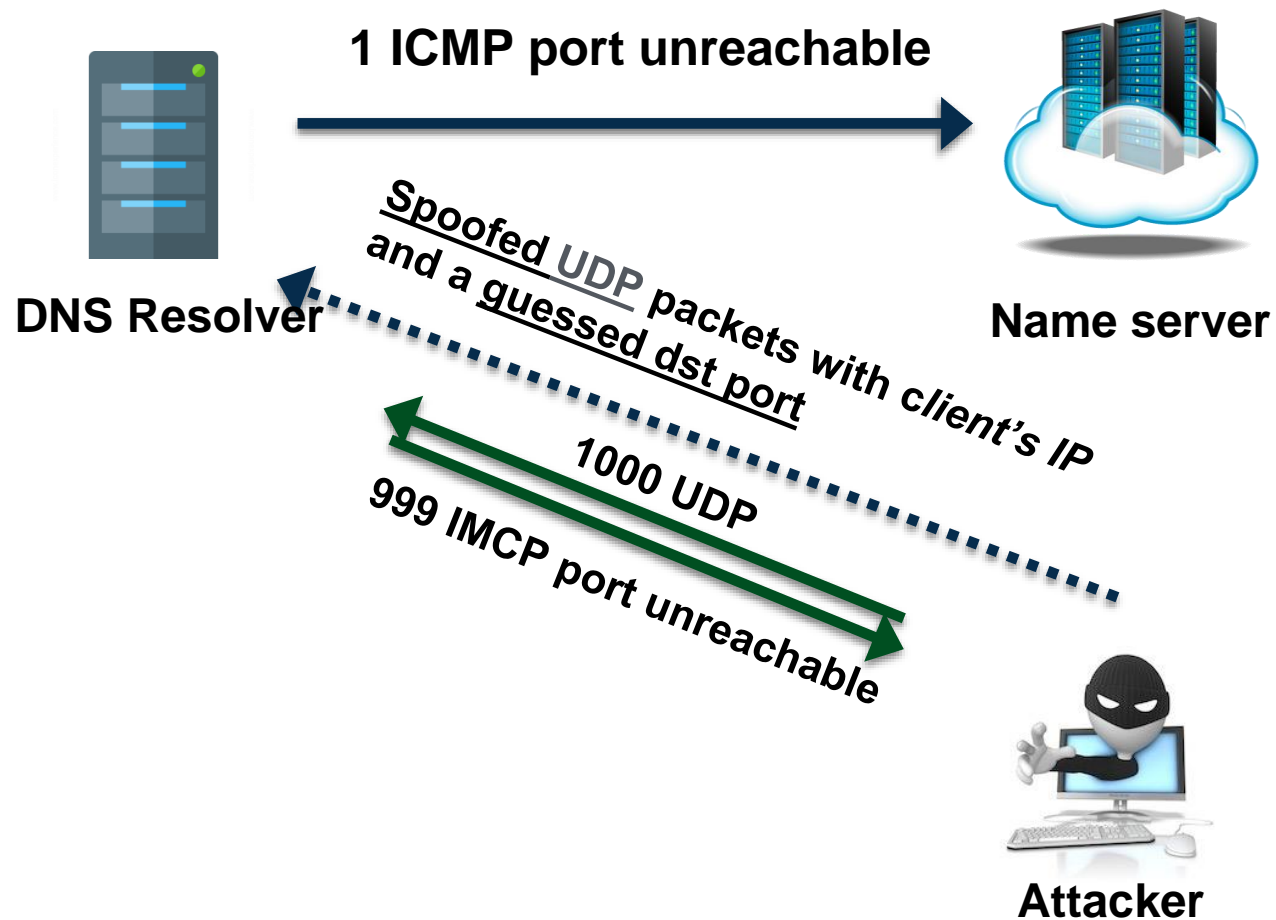
# Shared Resource: *Global* Rate Limit

- Since Linux 3.18
  - Outgoing ICMP global rate limit **shared** across all destinations
  - Default: ~1000 per second

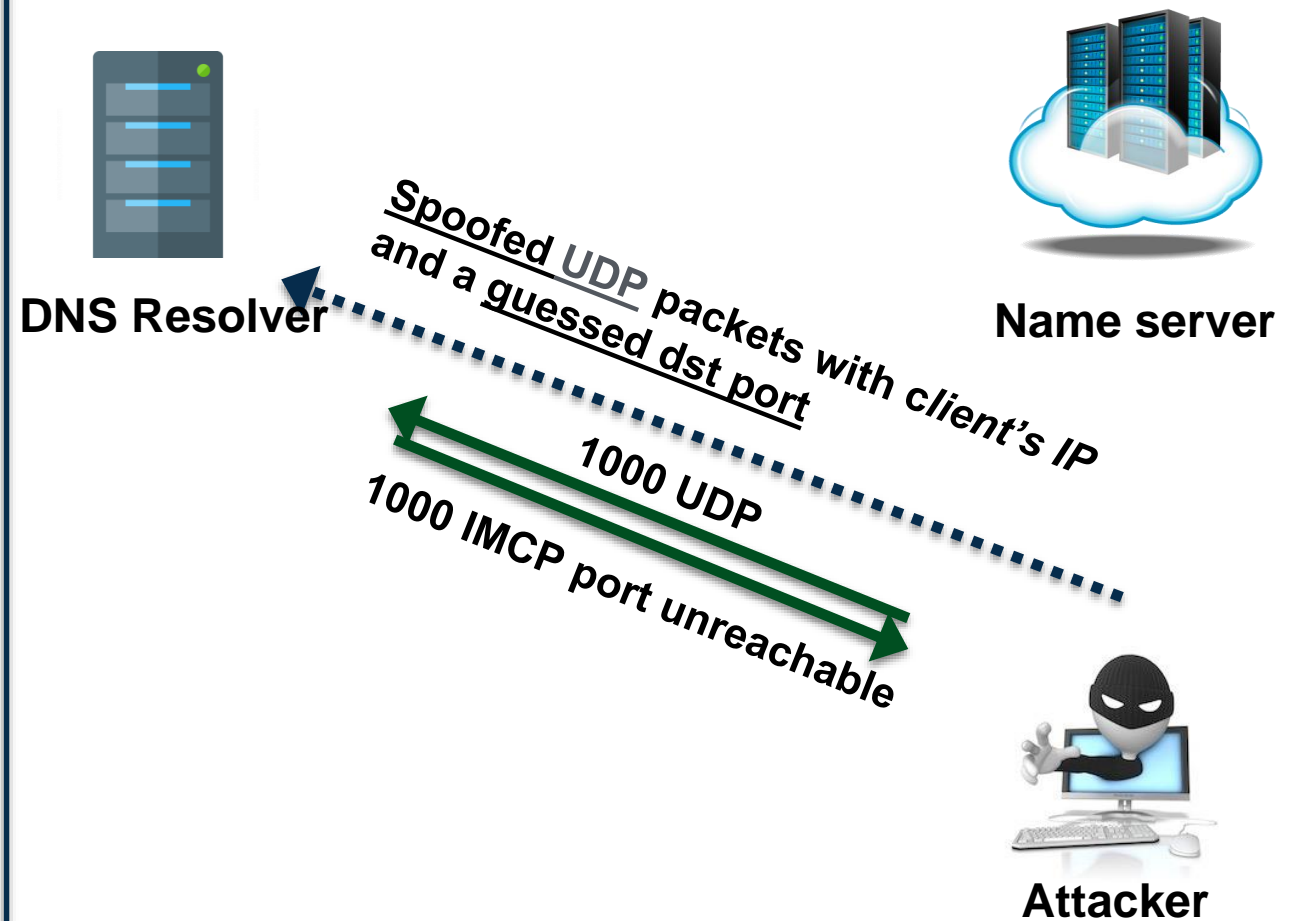


# Exploit the Vulnerability

- If it's a wrong guess:



- If it's a correct guess:





# Vulnerable DNS

## Open Resolvers:

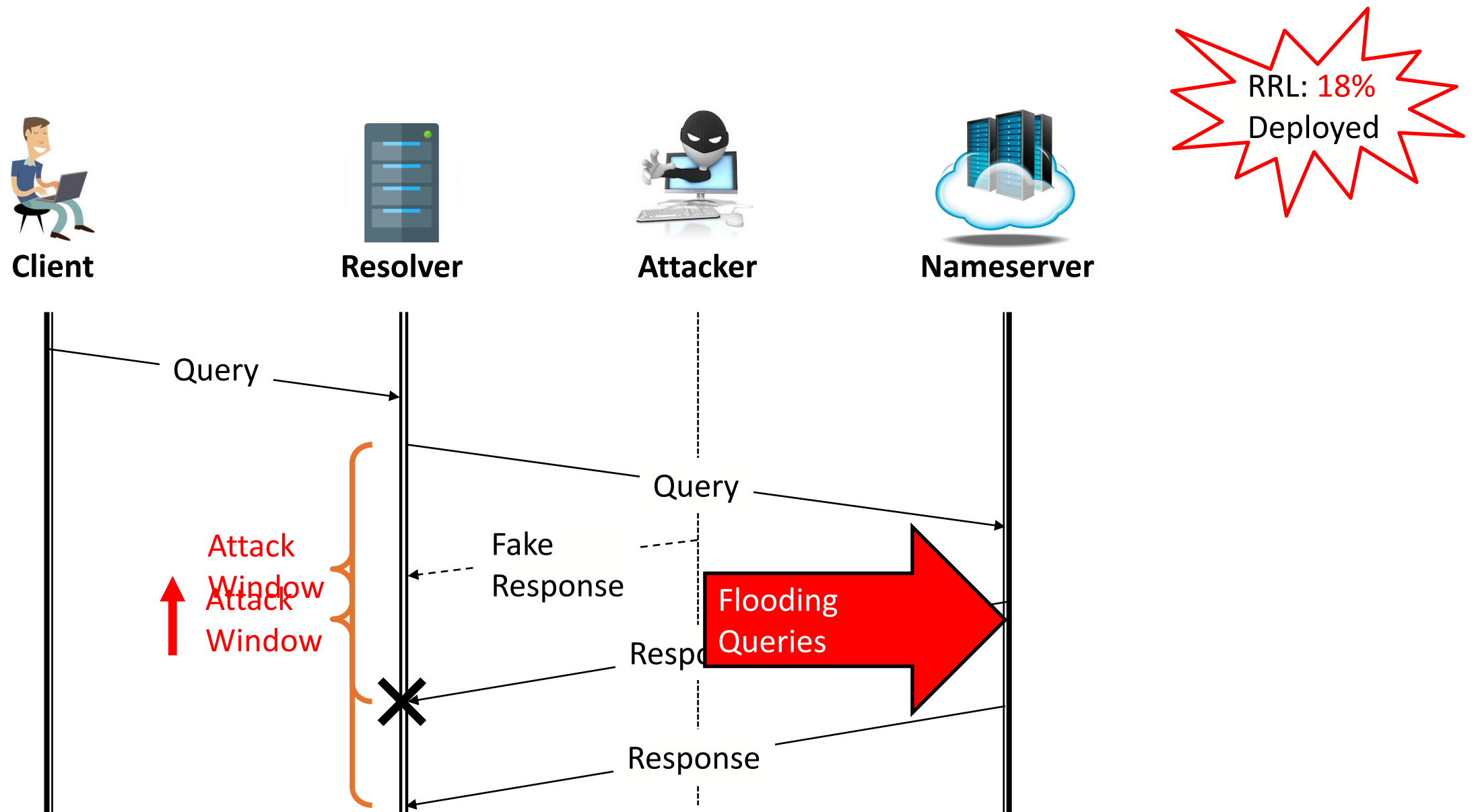
- **34%** Vulnerable

## • Well-known Public Resolvers:

- **12/14** Vulnerable

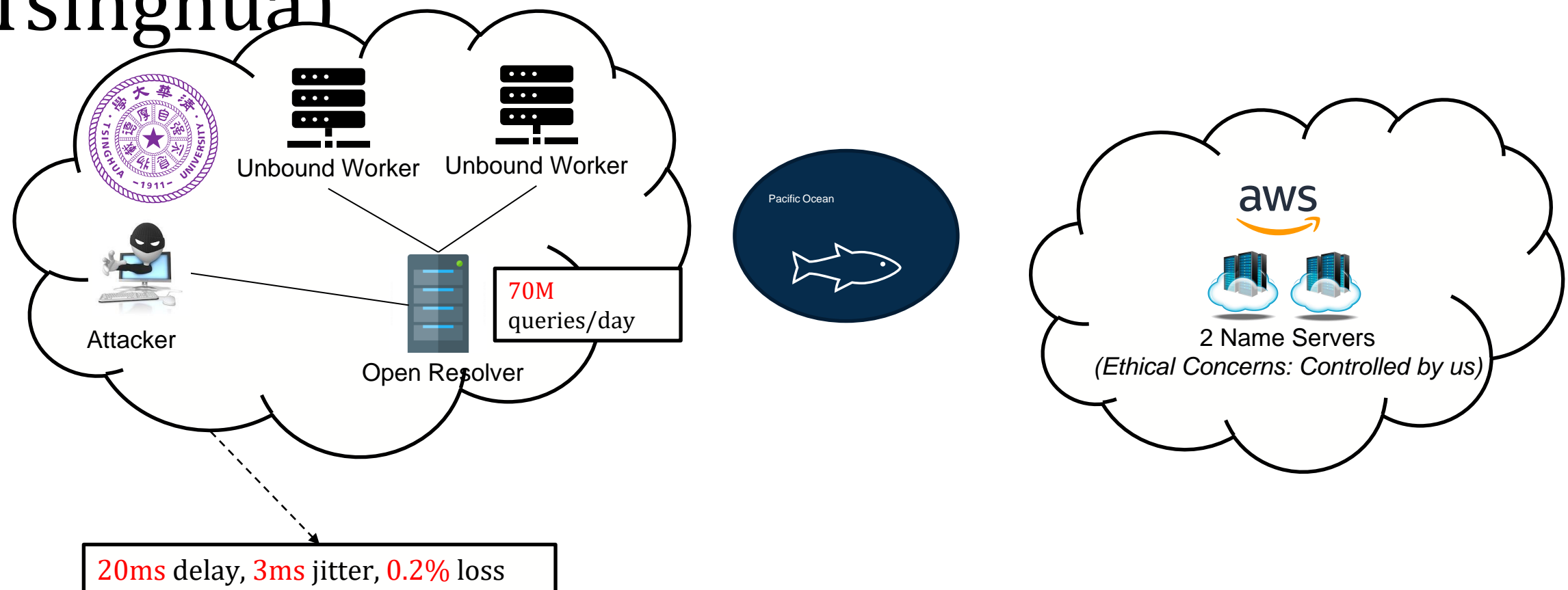
Google	8.8.8.8
Cloudflare	1.1.1.1
OpenDNS	208.67.222.222
Comodo	8.26.56.26
Dyn	216.146.35.35
Quad9	9.9.9.9
AdGuard	176.103.130.130
CleanBrowsing	185.228.168.168
Neustar	156.154.70.1
Yandex	77.88.8.1
Baidu DNS	180.76.76.76
114 DNS	114.114.114.114
Tencent DNS	119.29.29.29
Ali DNS	223.5.5.5

# Extend Attack Window



# Evaluation

- Setup 1: Production DNS resolver (in Tsinghua)



# 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
Commercial	4	1	2ms	30ms	0.6%	2.45 mins	1/1

# Questions

Reminder: ieval, homework2

