NUS | Computing
National University of Singapore

CS 4238: Computer Security Practice
Lecture-7: Network Attacks

Prasanna Karthik Vairam
Lecturer
Department of Computer Science
NUS School of Computing

Announcements

- Assignments
  - Assignment-1
    - 92/94 submitted. Evaluation in progress.
  - Assignment-2
    - On Network Attacks
    - Will be released tomorrow
- Labs
  - Lab 5 is on Network Attacks (later at 8.30 PM today)

Announcements

- Mid-term course feedback form
  - Will be circulated this week.
  - Hiccups: Support for Mac users (M1 and M2 chip) and problems with the setup. Getting the ITSEC lab ready for the mid-term
  - Hiccups: Slides are released late
  - On the bright side: Redesigning the lectures with more practical examples and industry readiness.
- Do remember that CS4238 is a work in progress. Thanks to your feedback, we will make it even better.

Network Attack Framework

What security attacks have you heard of in recent times?

Sea of Attacks

- Several **thousand attacks** are known in this space and several more are being discovered as we speak.
- How do we learn (or understand) all these attacks?
- An ***Attack framework*** helps us **place the attacks in context** and understand them with little effort.

Internet Users and Service Providers

Stakeholders of the Internet

- Victims: Alice, Bob, Carol

- Attackers: Mallory, Eve

Stakeholders of the Internet

Victim

Attacker

Adversaries

Who are the real-world Attackers who compromise our systems?

Start the presentation to see live content. For screen share software, share the entire screen. Get help at **pollev.com/app**

Who are the attackers?

- Alice □**Mallory** □ Bob
- Hackers: White hat, Black hat, Grey hat
- Organized Cyber Crime Organizations (e.g., Anonymous, Conti)
- Governments

Stakeholders of the Internet

victim

Attacker

Victims

Who are the real-world victims?

Start the presentation to see live content. For screen share software, share the entire screen. Get help at **pollev.com/app**

Who are the victims?

- Subtle difference between collateral damage and victims of attacks.
- Collateral Damages:
  - Low profile people (You and me ☺️)
  - IoT Devices
  - Routers on the internet
  - Unattended servers on the Internet (Jet Airways)
- Victims of Attacks:
  - High profile people
  - High profile Organizations (e.g., Google, Microsoft)
  - Governments

Mind Map of Attackers and Victims

When poll is active, respond at **pollev.com/prasanna**

As an Attacker, which one of the following do you compromise?

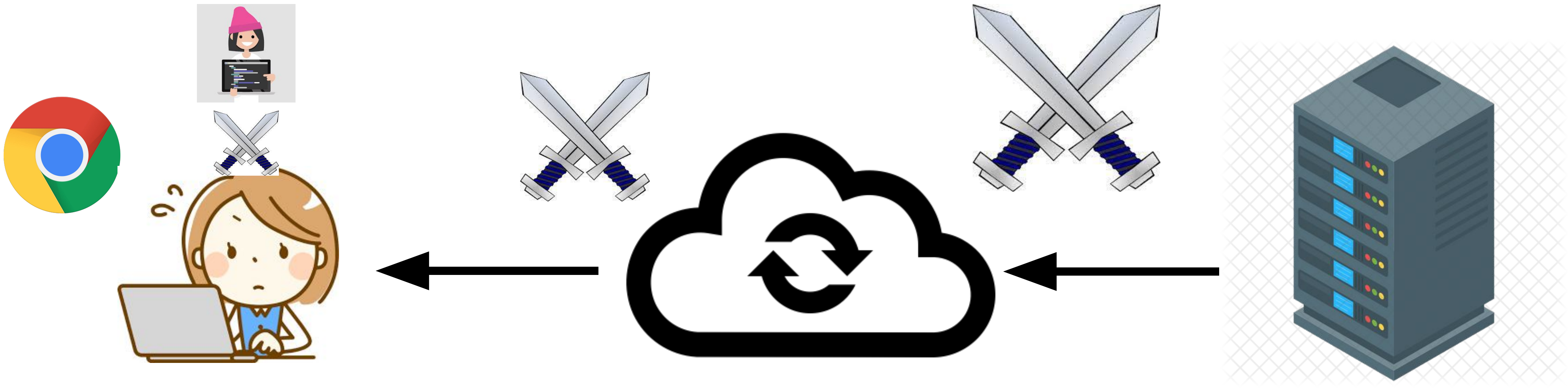
Client Machines

Network Router

Servers

Victim-Attacker Combination

Victim: Web clients like you and me!



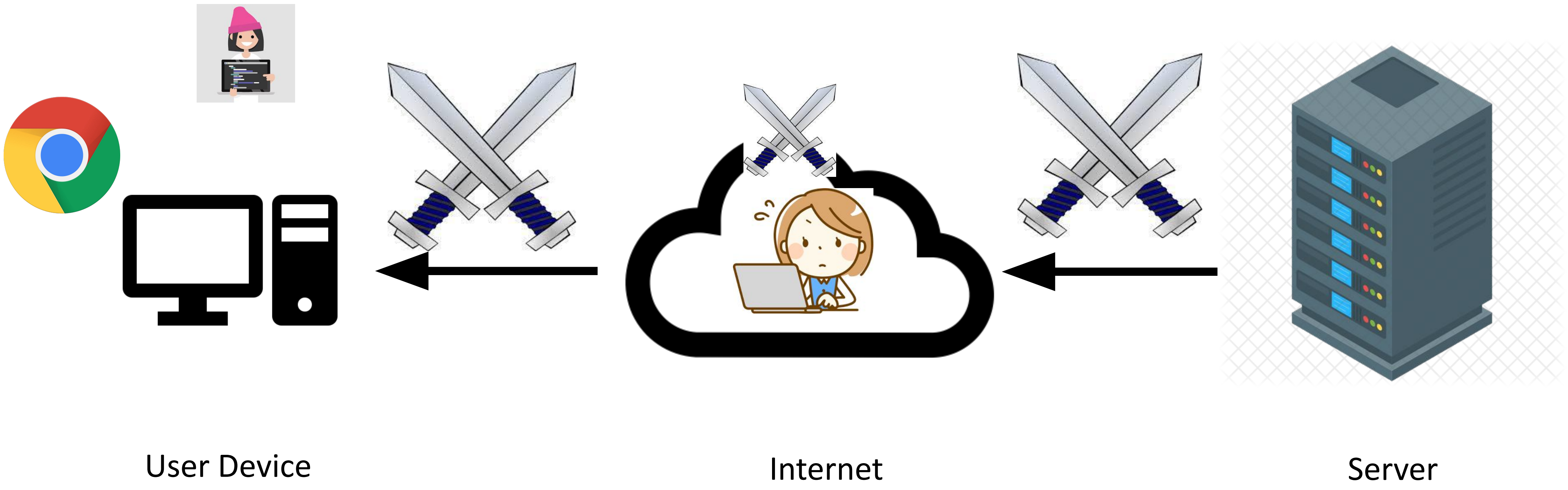
User Device

Internet

Server

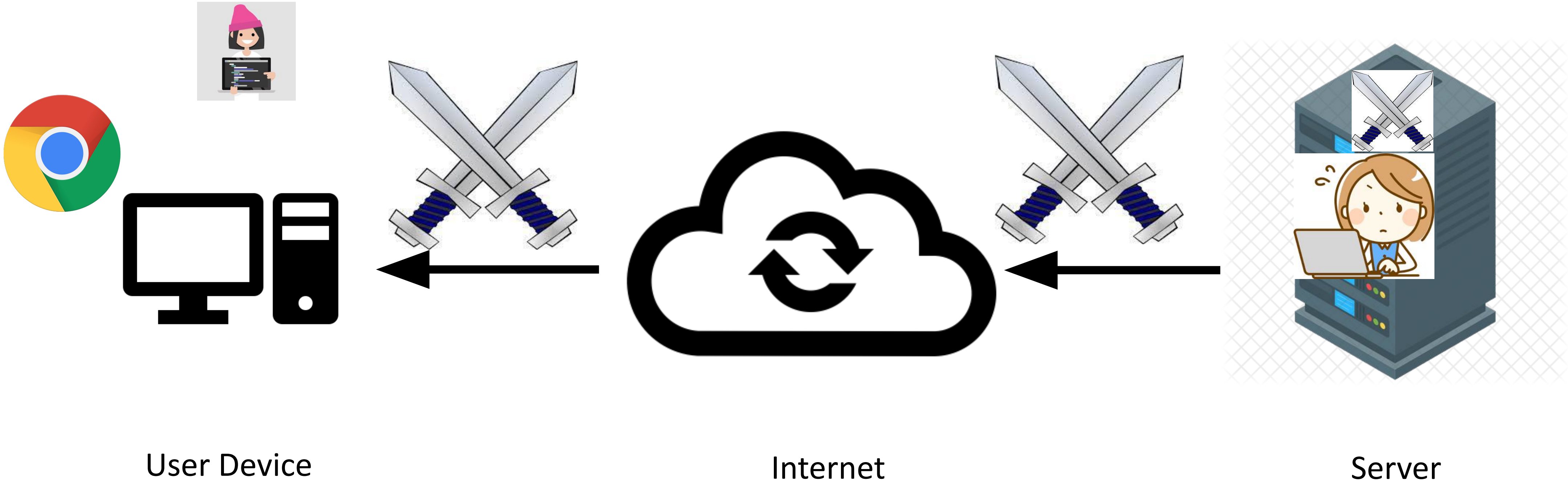
Victim-Attacker Combination

Victim: Internet Service Providers and DNS providers.



Victim-Attacker Combination

Victim: Companies like Youtube, Netflix, etc.



Attacker Goals and Objectives

Attacker’s Objectives

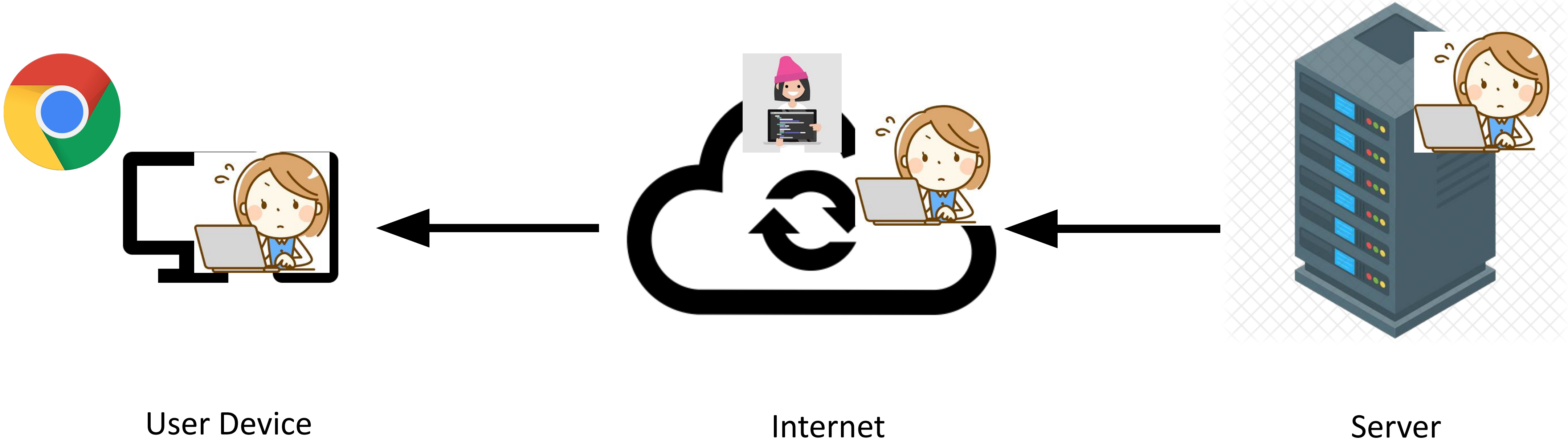
- To compromise an Internet router
- To compromise the server
- Launch a Denial of Service Attack
- Perform traffic analysis on encrypted traffic

Attacker’s Goals

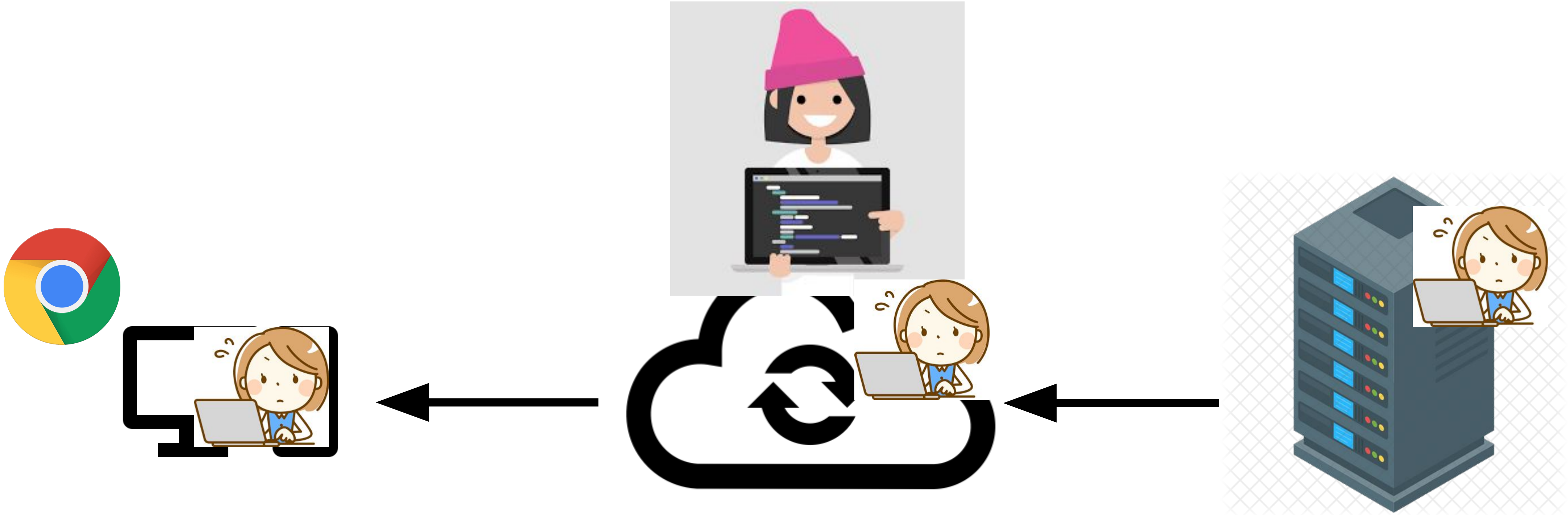
- Deny service to cause business loss.
- Censorship (selective denial)
- Eavesdropping
- Impersonation
- …

Framework for Network Attacks

Option 3: Victim-Attacker Combination



Our Setup for this Lecture



User Device

Internet

Server

Adversary Model

What can the adversary do after gaining control over an Internet Router?

Adversary Capability

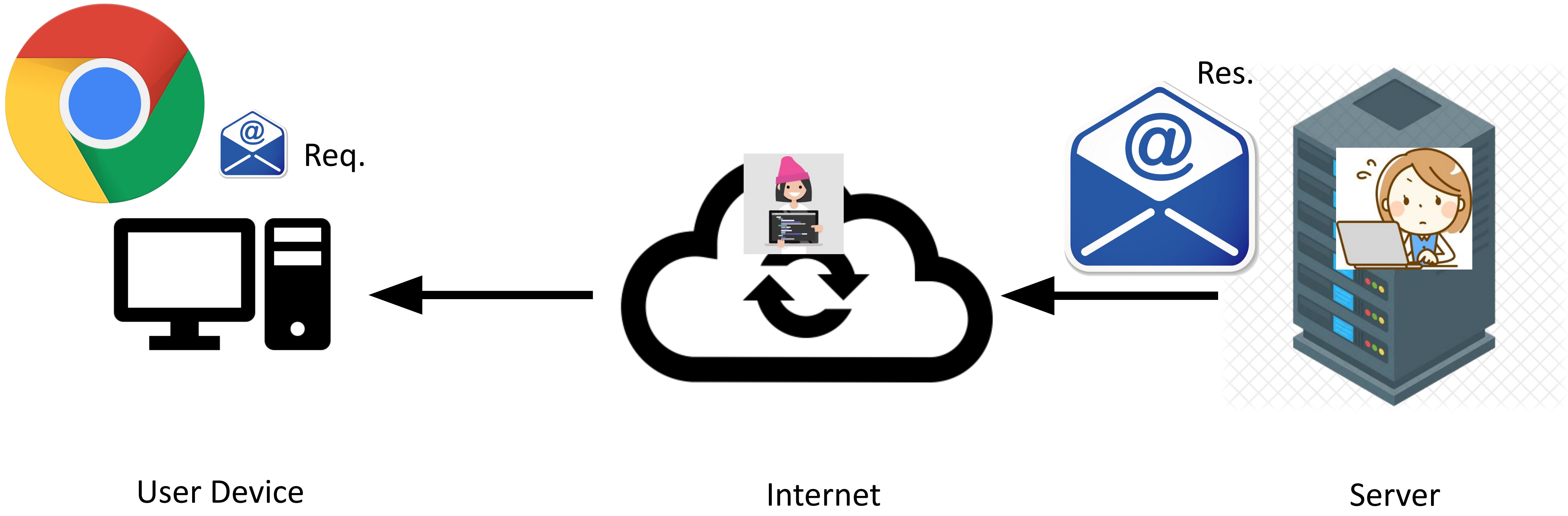
- Passive Attacks
  - Stealthy but most attacks only reveal basic information.
  - Eavesdropping/Sniffing Traffic
- Active Attacks
  - More powerful but possibility of getting caught is high.
  - Packet Dropping
  - Packet Injection
  - Packet Delay
  - Packet Modification

In the real world, what are the capabilities of an attacker?

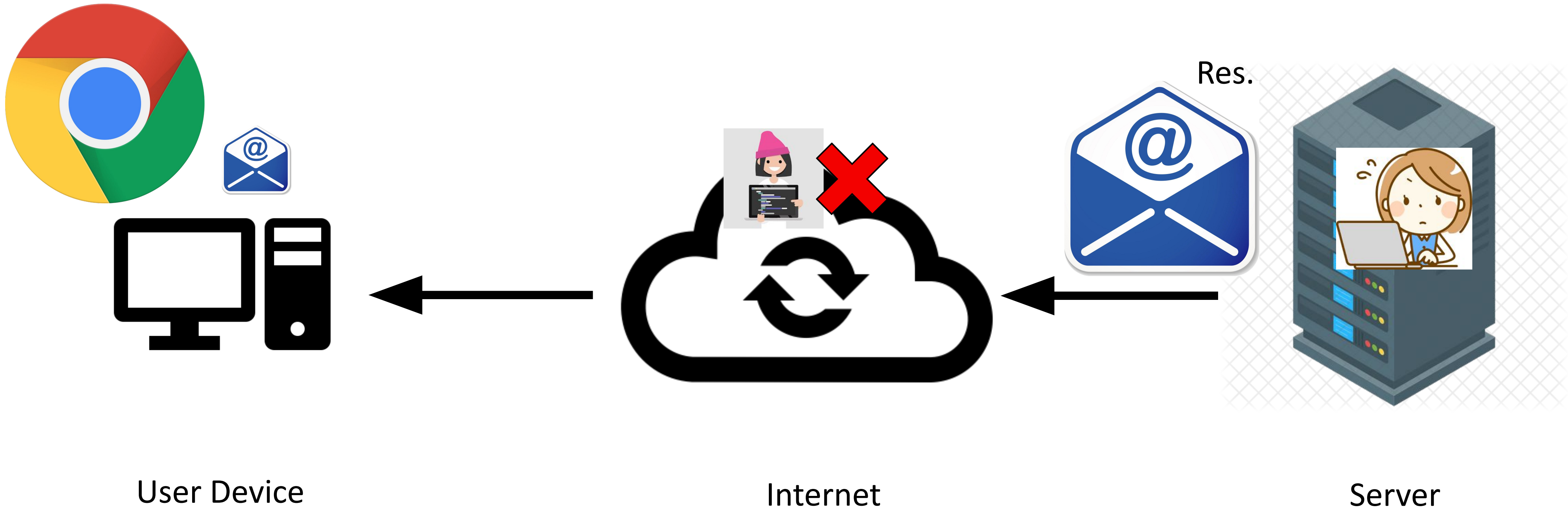
- Depends on the device that the attacker has control over
- Case 1: User level access to router
- Case 2: Root access to router
- Attacker Goals should measure up to the Attacker Capabilities!
- E.g., identifying user password on plaintext traffic is not a valid attack!

Denial of Service Attacks

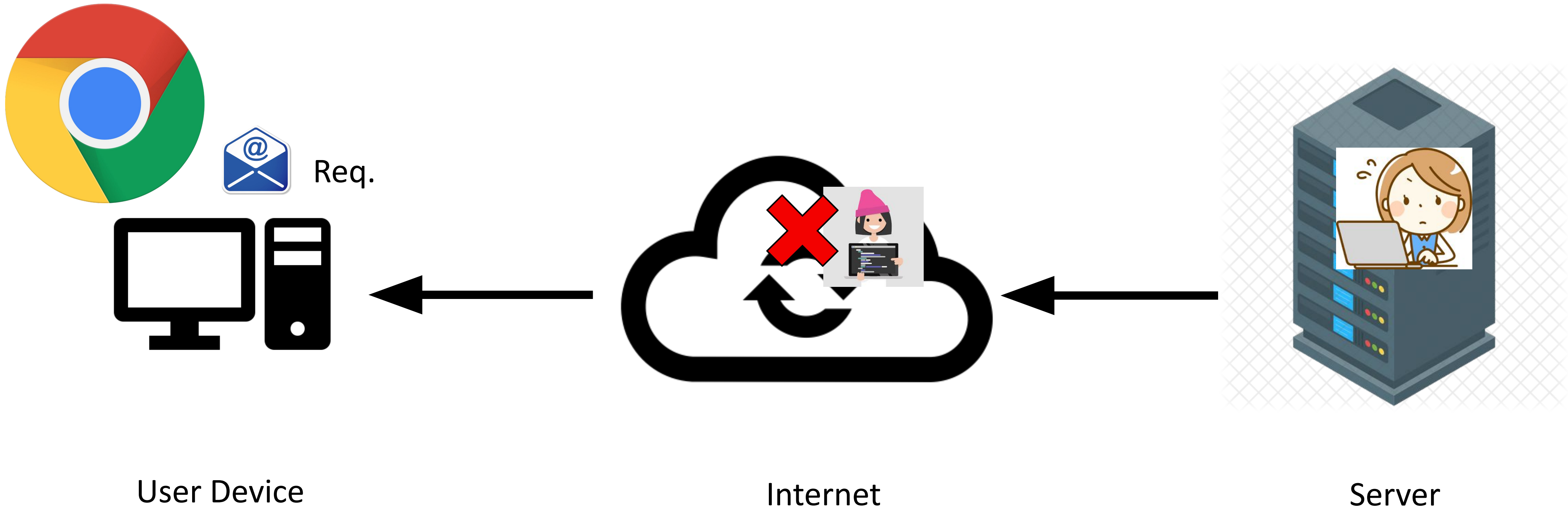
Basics of DoS Attacks



Basics of DoS Attacks

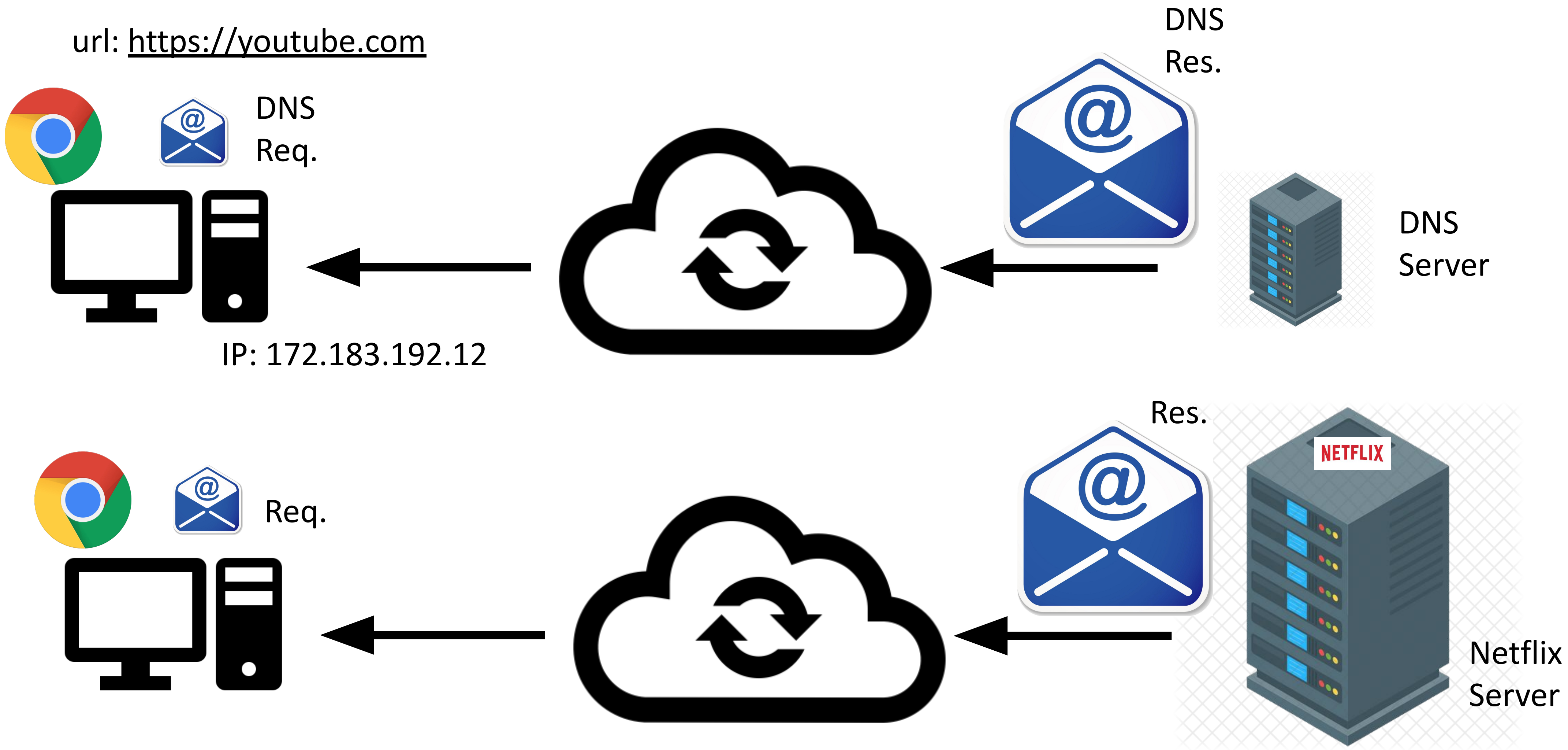


Basics of DoS Attacks

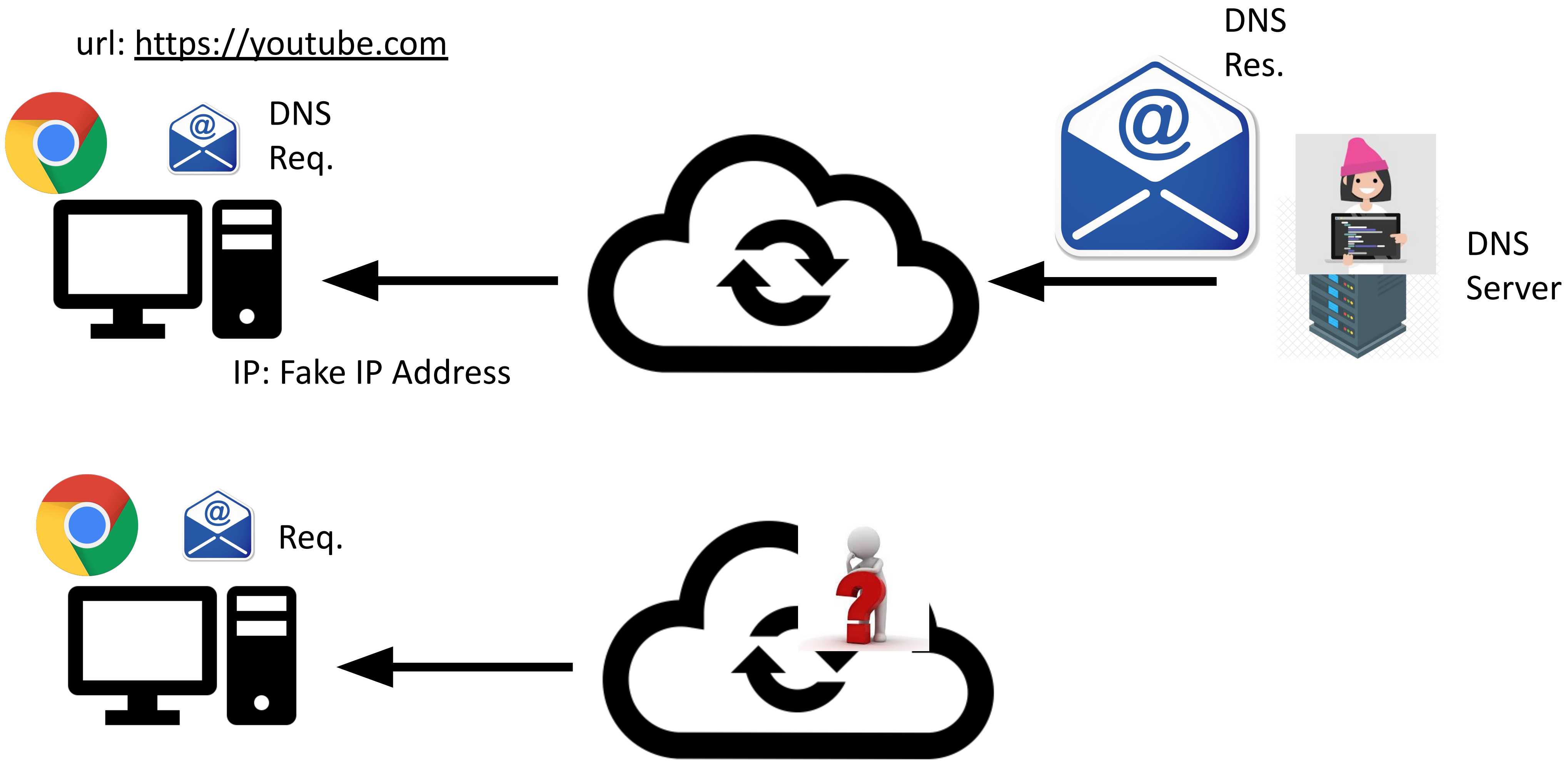


Network-based DoS Attack

Network DoS Attack #1: DNS Blackhole



Network DoS Attack #1: DNS Blackhole



url: https://youtube.com

DNS Req.

DNS Res.

DNS Server

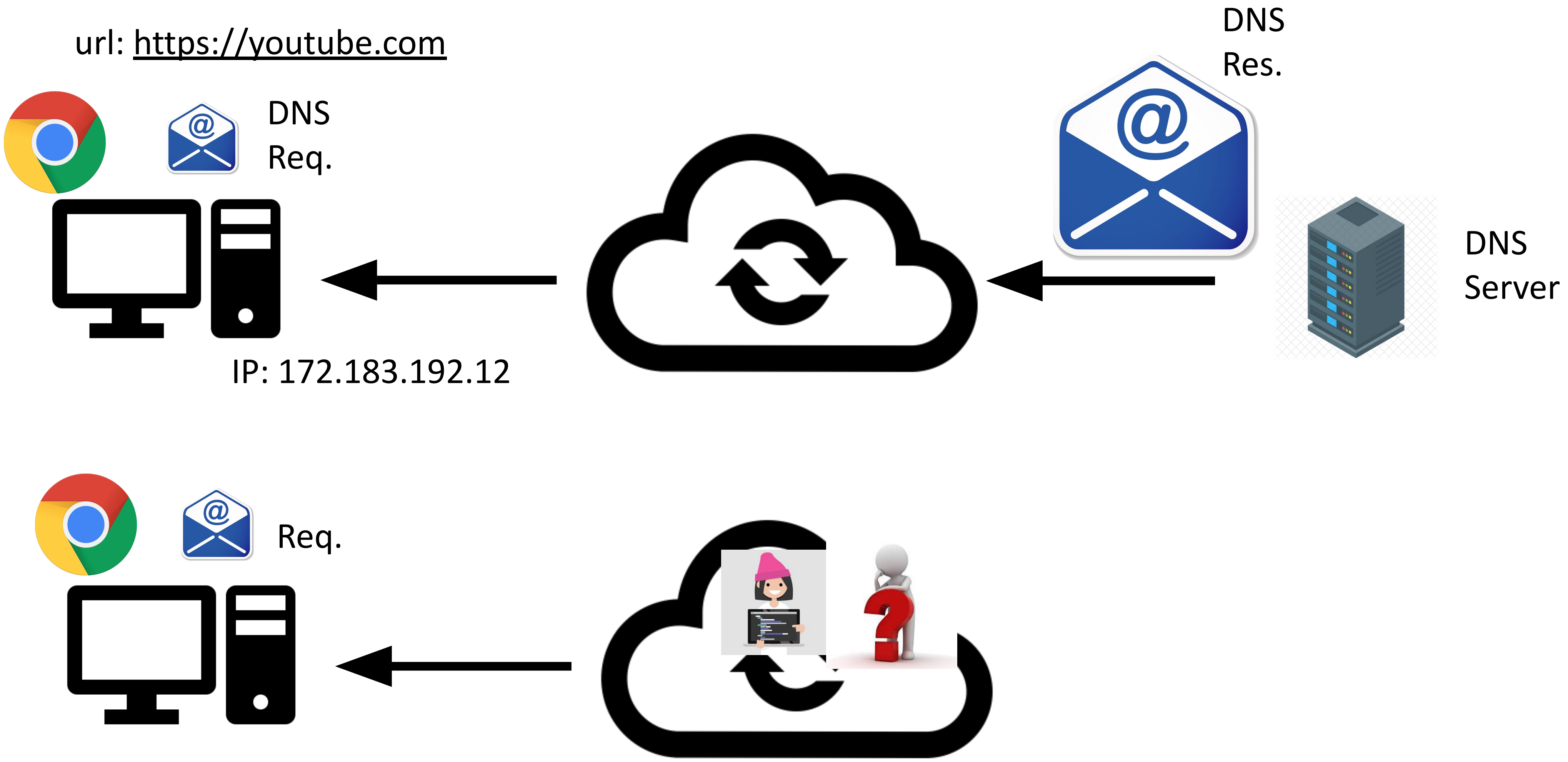
IP: Fake IP Address

Req.

What routing protocols are you familiar with?

Start the presentation to see live content. For screen share software, share the entire screen. Get help at **pollev.com/app**

Network DoS Attack #2: BGP Routing Blackhole



url: https://youtube.com

DNS Req.

IP: 172.183.192.12

DNS Res.

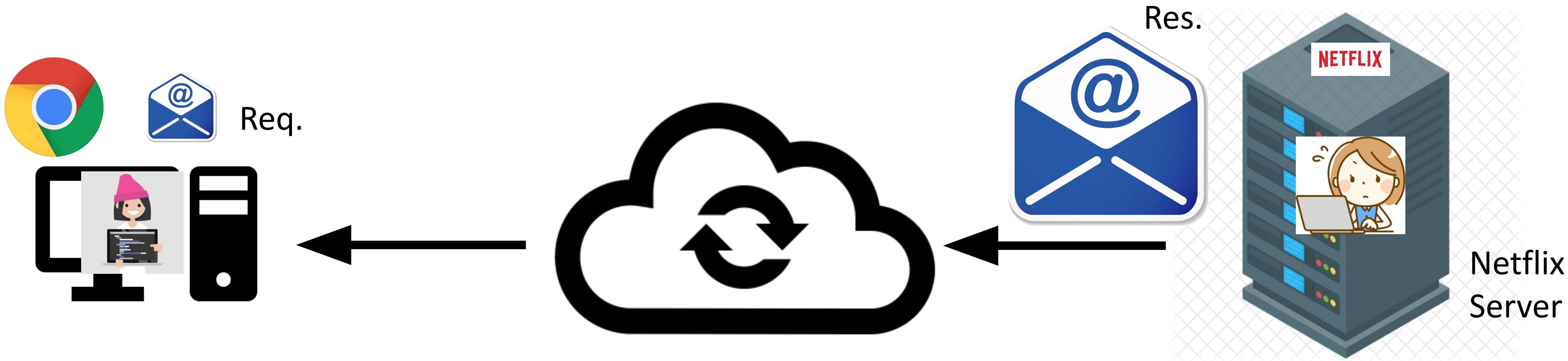
DNS Server

Req.

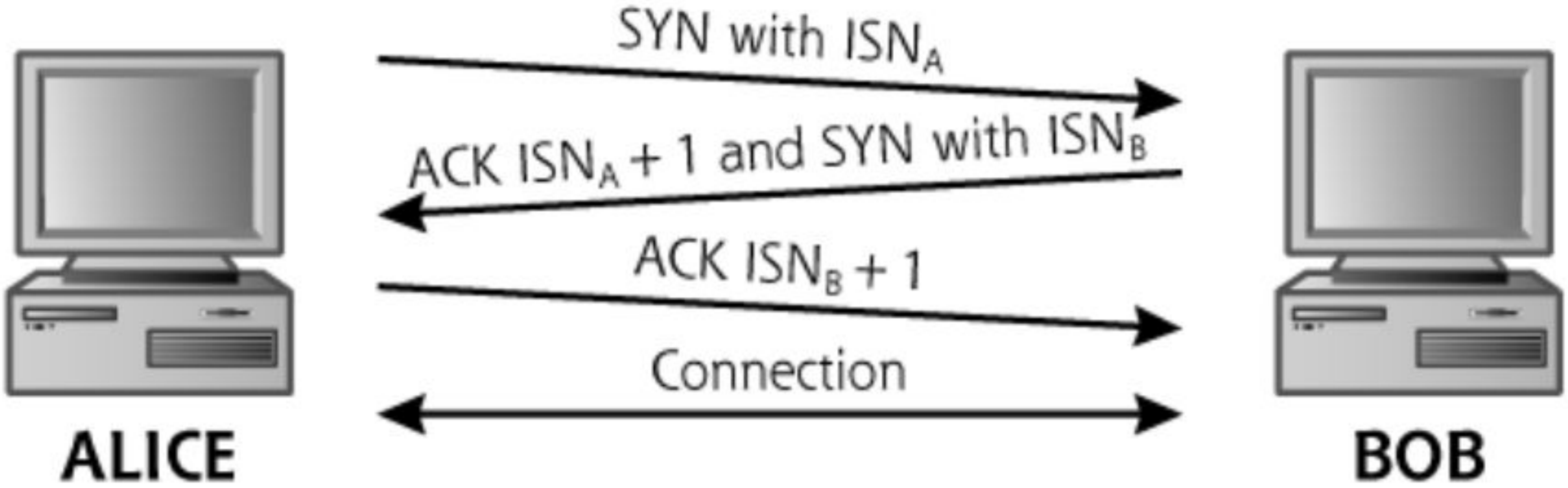
Key Idea: IP Address is correct but the routing table is fudged!

Server-based DoS Attack

Server-based DoS Attack: TCP SYN Flood Attack

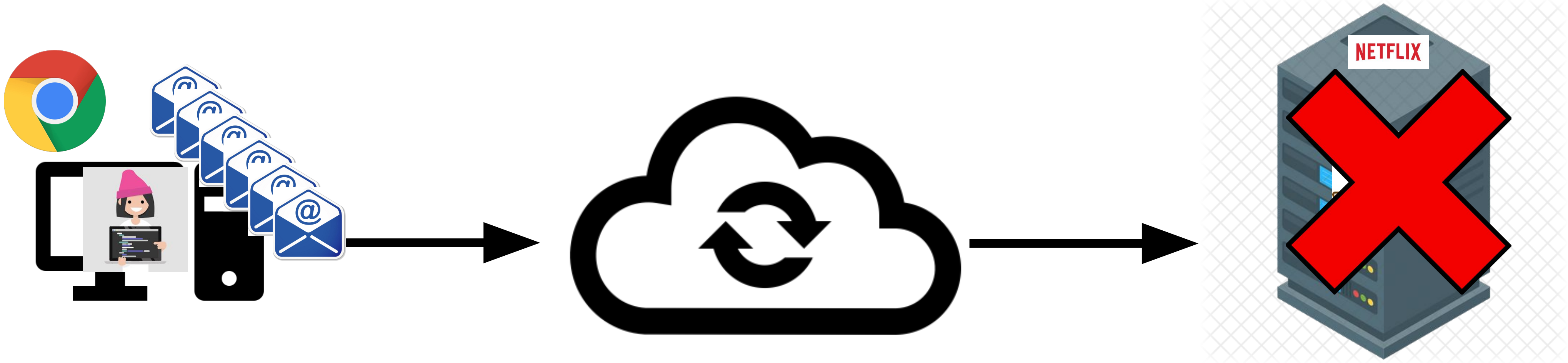


TCP Connection Setup

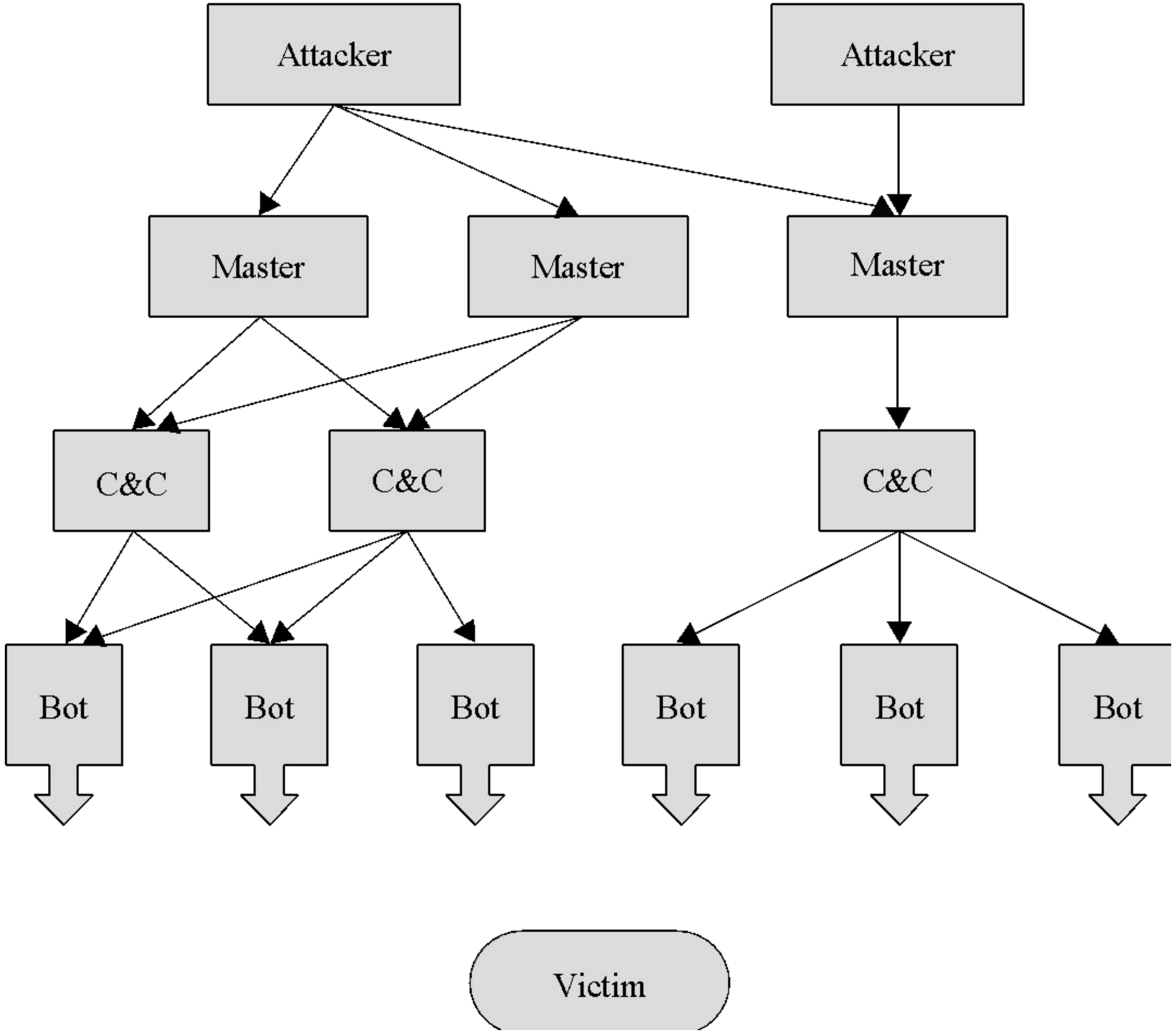


Key Idea: Each connection setup creates several MB of states at Bob (Server)

Server-based DoS Attack: TCP SYN Flood Attack

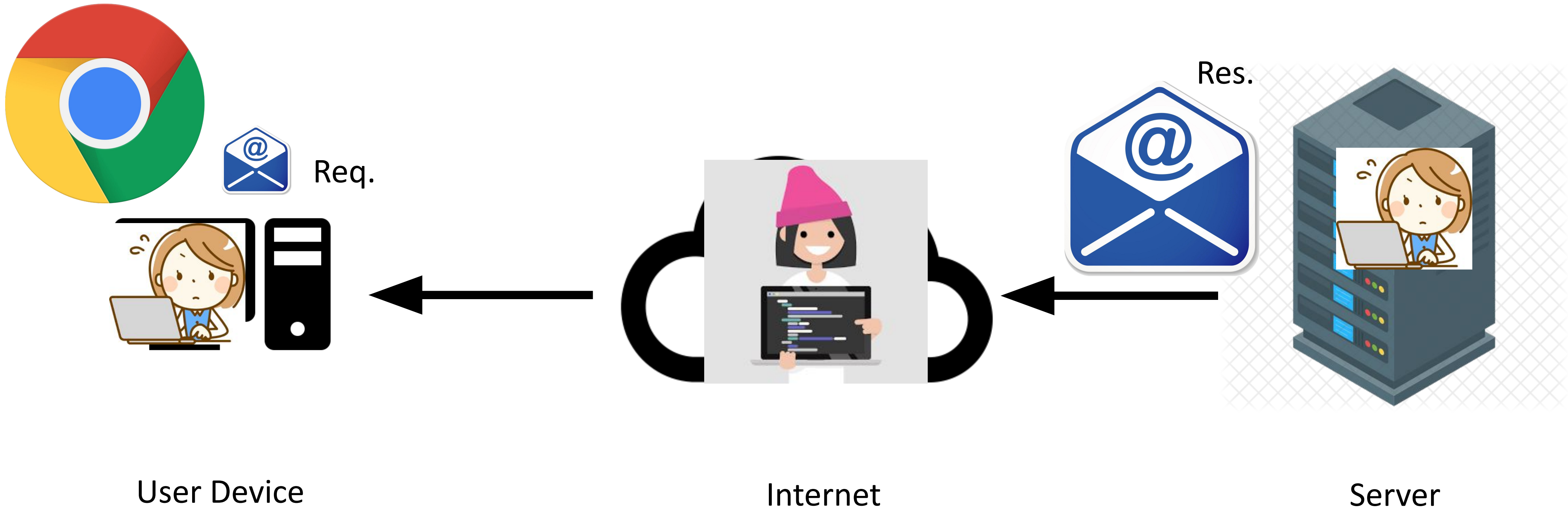


Distributed DoS (DDoS) Attacks

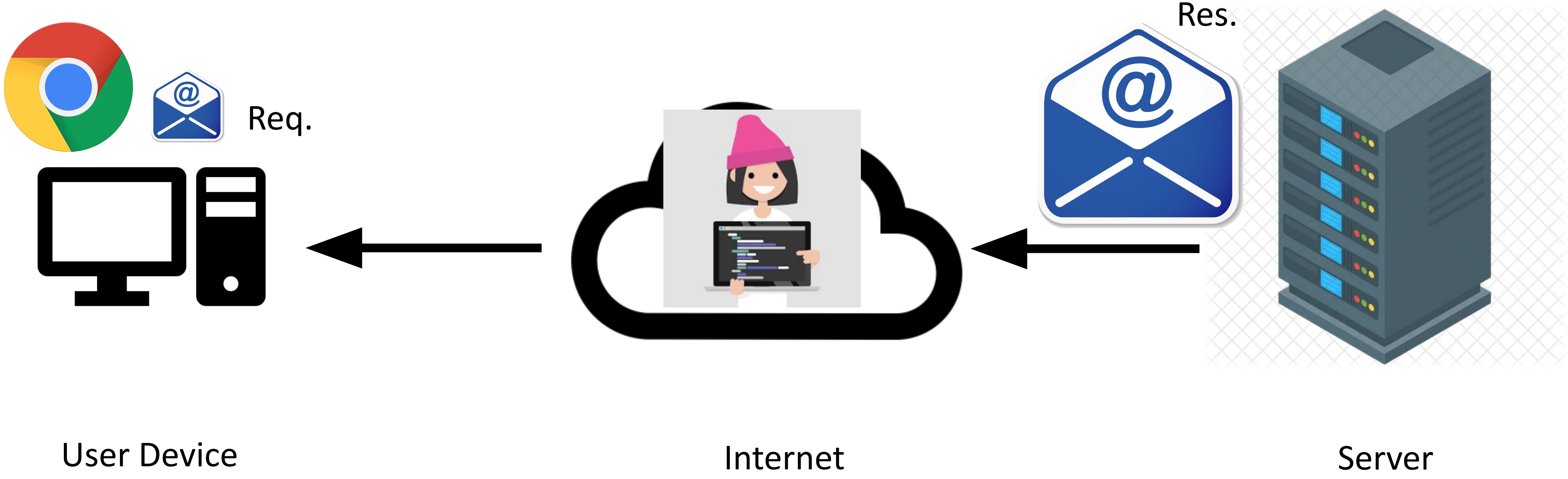


Passive Attacks

Sniffing Attack

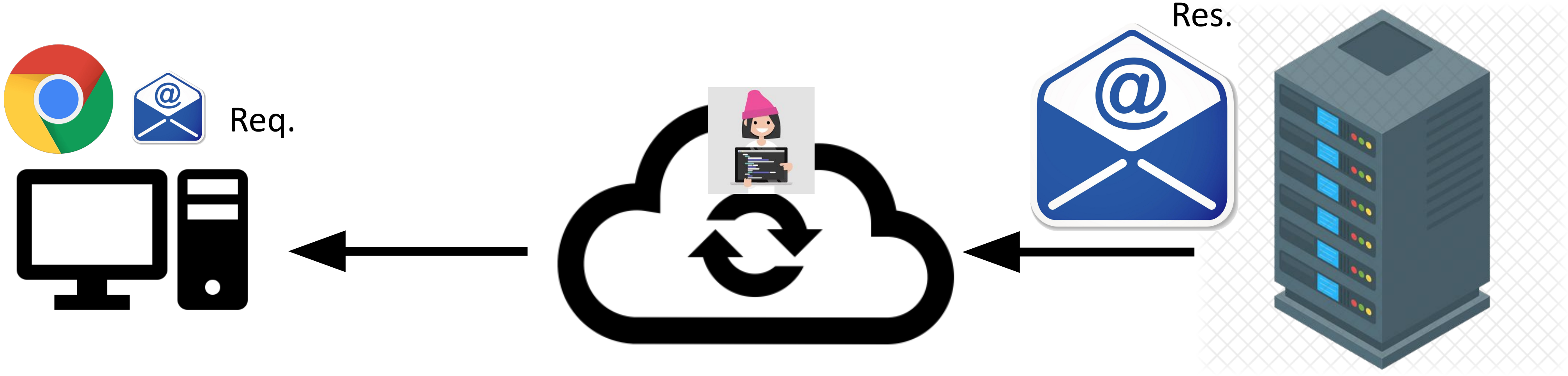


Plaintext Traffic Analysis



Key Idea: Sniffing Reveals the data (payload) exchanged!

Encrypted Traffic Analysis



User Device

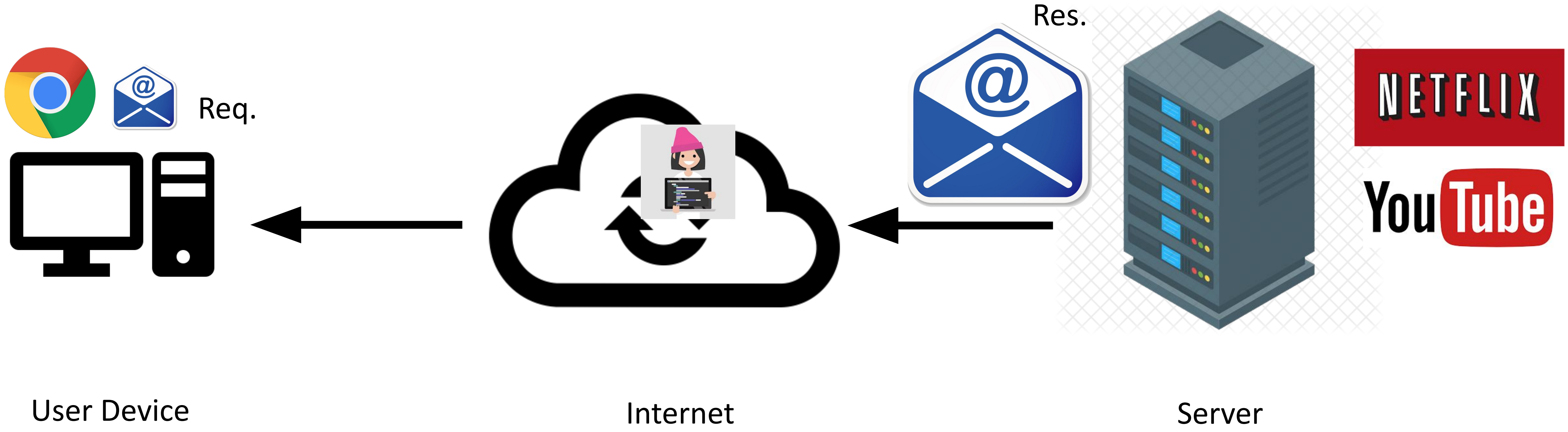
Internet

Server

Key Idea: Data (payload) is not visible to the attacker!

When Traffic is Encrypted, Is there any use of performing an eavesdropping attack?

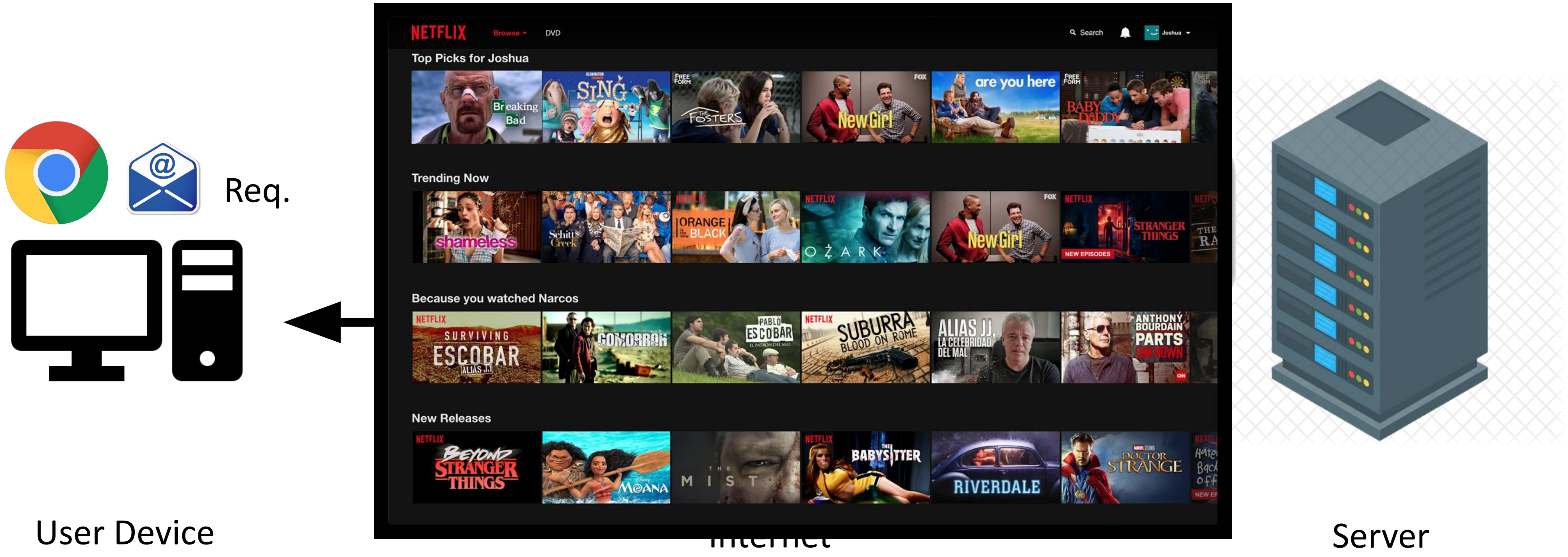
ETA Attacks Stage-I: Revealing the Website Accessed



Key Question: Is the victim accessing Youtube or Netflix?

How? Look at the destination IP address of the packets

ETA Attacks Stage-II: Revealing the Video Watched

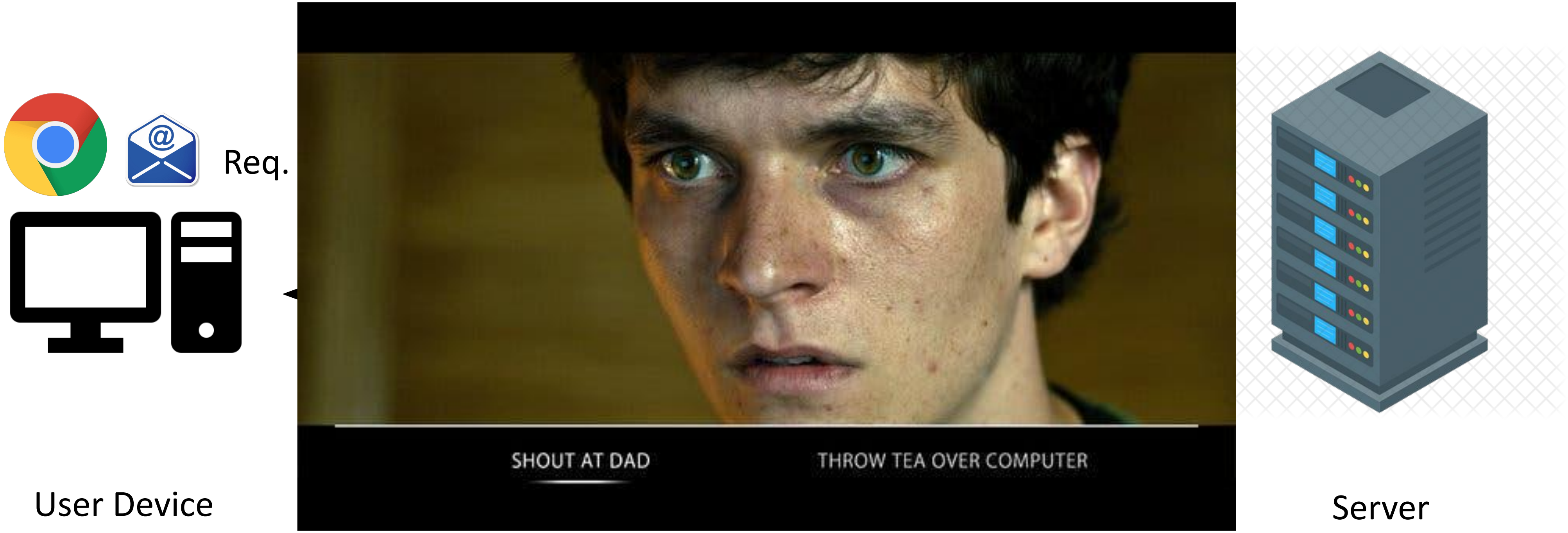


Key Question: Which Netflix video is the victim accessing?

How? IP addresses of different videos downloaded are the same

Key Idea: Different videos have different sizes of resources!

ETA Attacks Stage-III: Revealing the Video Choices Made



Req.

User Device

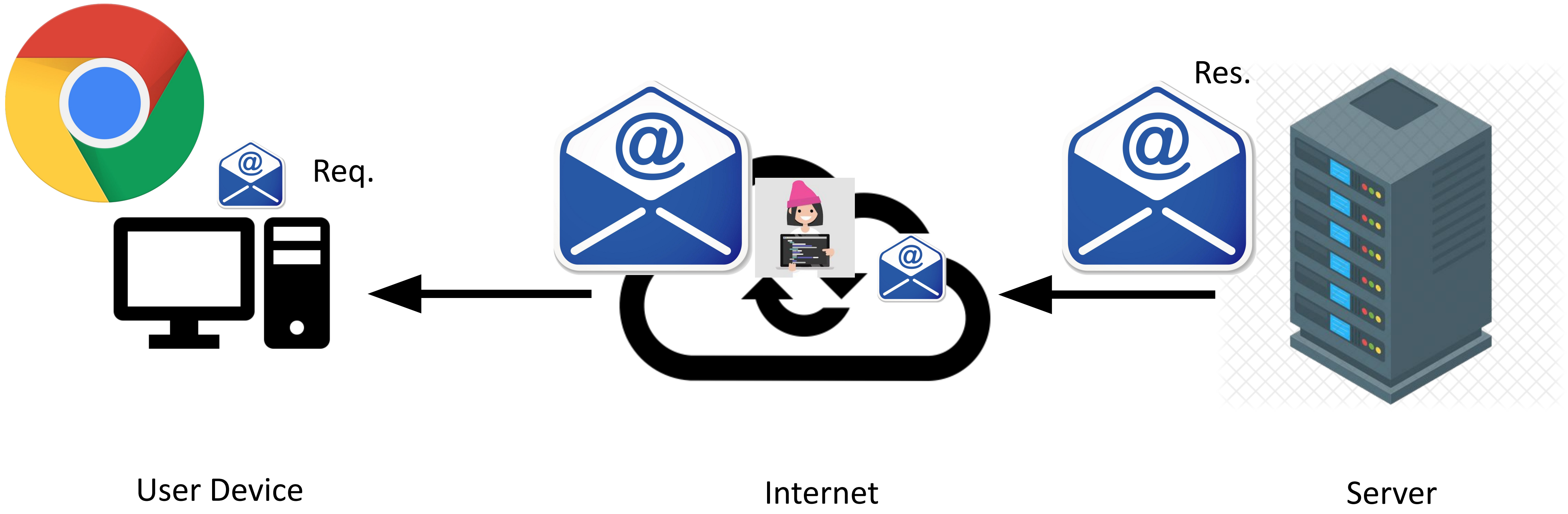
Server

Key Question: Which Netflix Interactive video choice is the victim making?

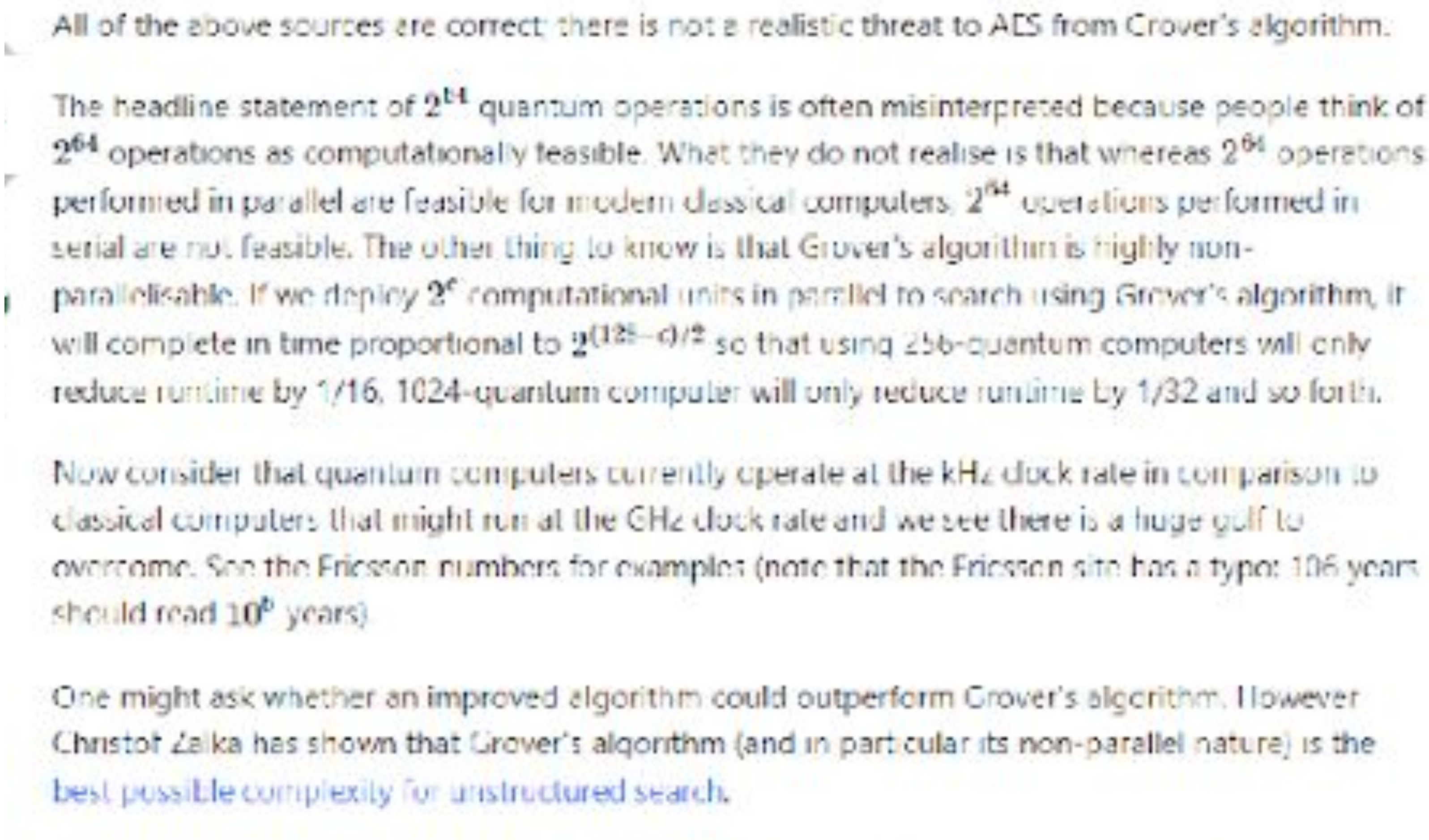
How? Let us see…

Passive + Active Attacks

MiTM: Breaking Encryption



MiTM: Breaking Encryption



All of the above sources are correct; there is not a realistic threat to AES from Grover's algorithm.

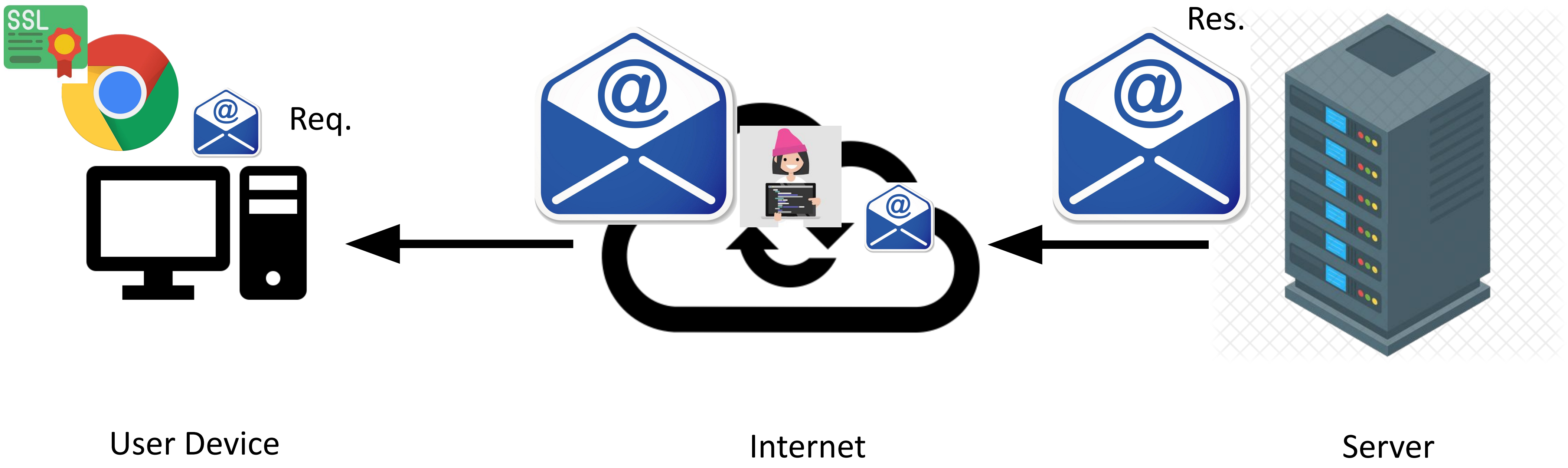
The headline statement of 2^{64} quantum operations is often misinterpreted because people think of 2^{64} operations as computationally feasible. What they do not realise is that whereas 2^{64} operations performed in parallel are feasible for modern classical computers, 2^{64} operations performed in serial are not feasible. The other thing to know is that Grover's algorithm is highly non-parallelisable. If we deploy 2^{c} computational units in parallel to search using Grover's algorithm, it will complete in time proportional to $2^{(128-c)/2}$ so that using 256-quantum computers will only reduce runtime by 1/16, 1024-quantum computer will only reduce runtime by 1/32 and so forth.

Now consider that quantum computers currently operate at the kHz clock rate in comparison to classical computers that might run at the GHz clock rate and we see there is a huge gulf to overcome. See the Ericsson numbers for examples (note that the Ericsson site has a typo: 106 years should read 10^{6} years)

One might ask whether an improved algorithm could outperform Grover's algorithm. However Christof Zalka has shown that Grover's algorithm (and in particular its non-parallel nature) is the best possible complexity for unstructured search.

MiTM: Fake SSL Certificates

Link: https://www.f5.com/labs/articles/threat-intelligence/kazakhstan-attempts-to-mitm-itscitizens



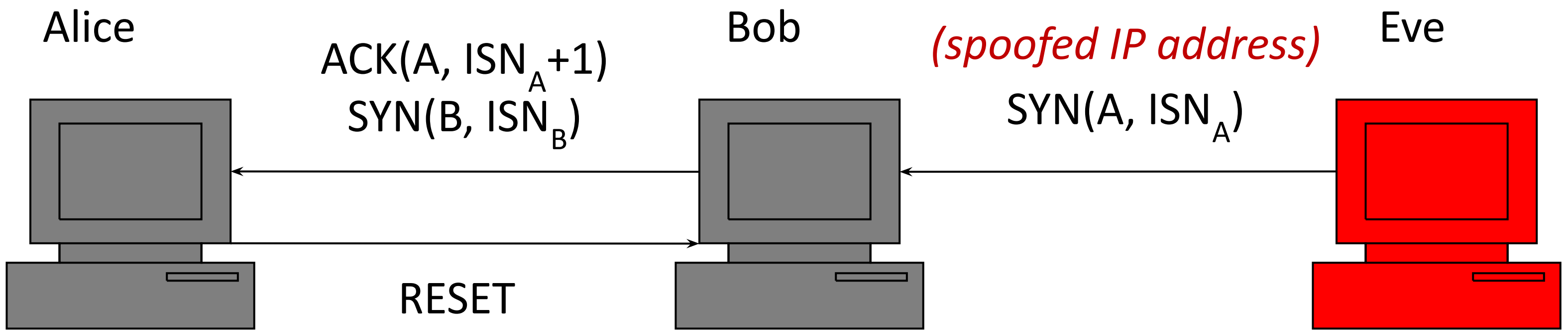
Next Best thing…

- Packet sniffing
- Packet Dropping
- Packet Injection
- Packet Modification
- Packet Delay

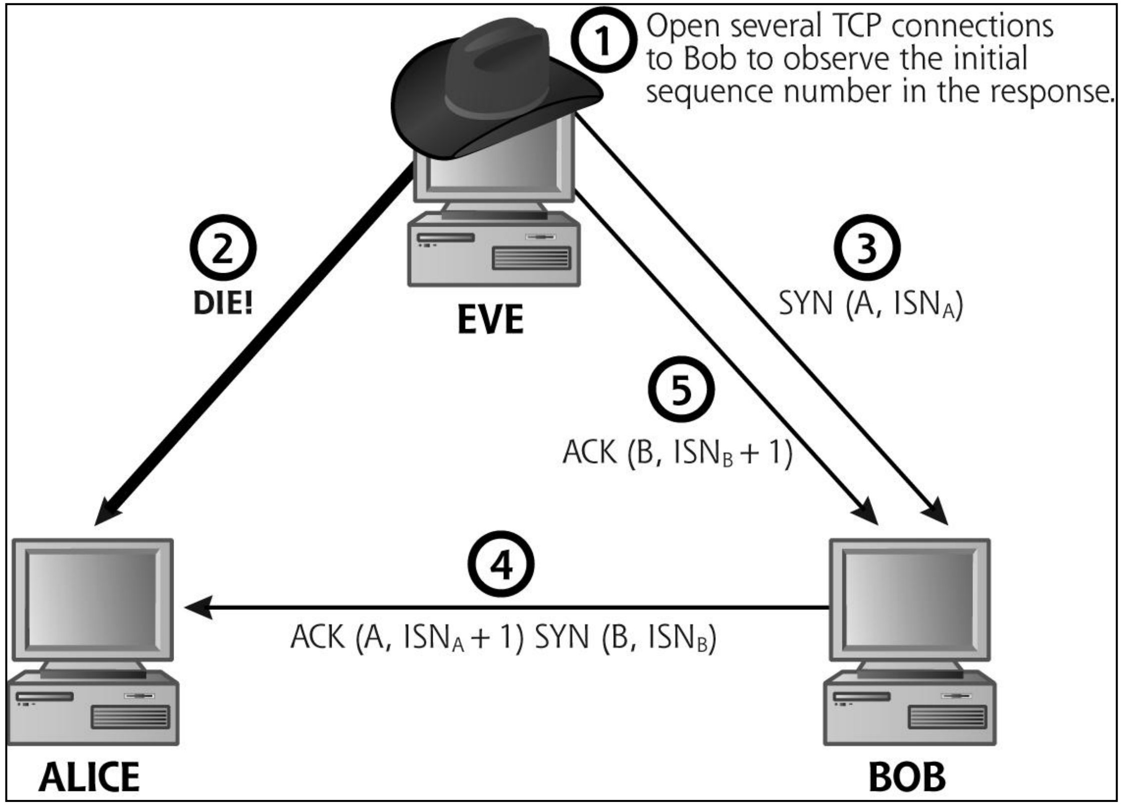
Attack I: IP Spoofing Attack

- Simple/basic **spoofing**:
  - Change your host’s source IP address with a **spoofed IP address** to hide your actual IP address
  - Even simpler: create packets with desired IP addresses using a **tool** such as: Netwox, Hping2, Nemesis, NetDude
- Problem: Eve **can’t** receive the response packets!
  - A one-way traffic only
  - But it works if Eve is **on the same LAN**, and sniff Bob's response
  - To prevent Reset packets from Alice? DoS her!

Attack I: IP Spoofing Attack

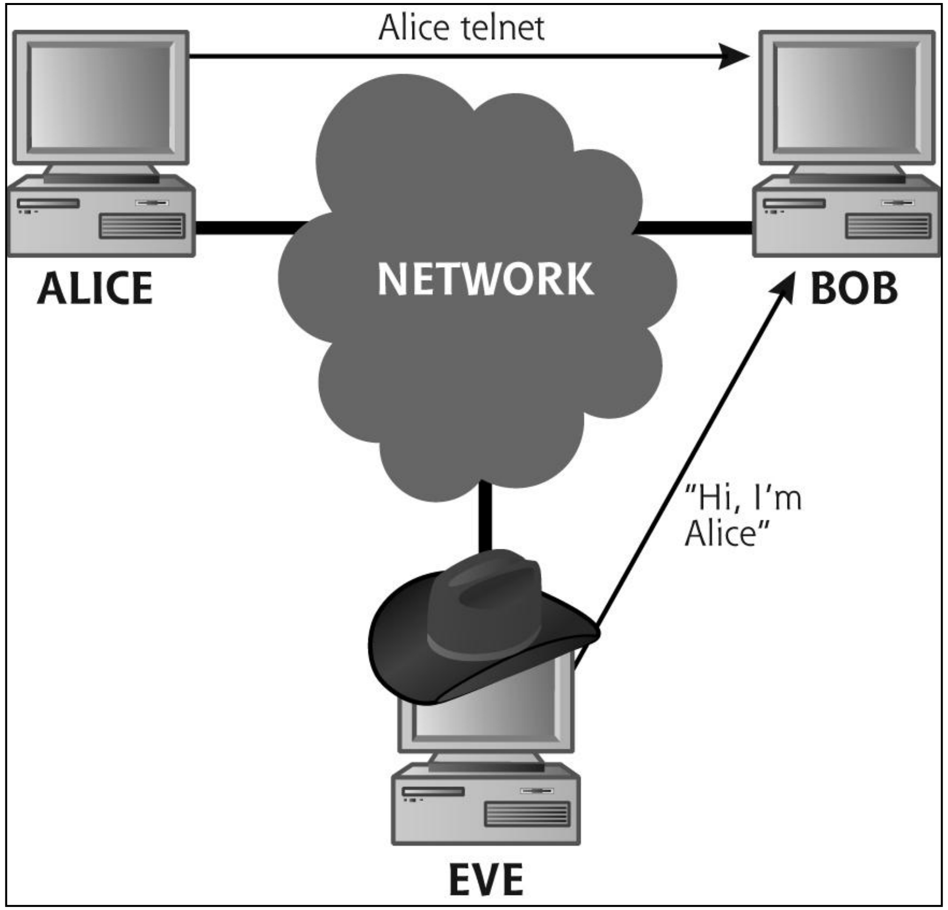


Attack I: IP Spoofing Attack


1 Open several TCP connections to Bob to observe the initial sequence number in the response.
2 DIE!
EVE
3 SYN (A, ISN$_A$)
5 ACK (B, ISN$_B$ + 1)
4 ACK (A, ISN$_A$ + 1) SYN (B, ISN$_B$)
ALICE
BOB

Attack II: Session Hijacking Attack

- Combination of **sniffing** and **spoofing**
- E.g. Alice has a telnet session with Bob
- Eve can sniff the connection between Alice and Bob
- Eve spoof a packet with: Alice's IP address as the source IP and the correct TCP sequence no

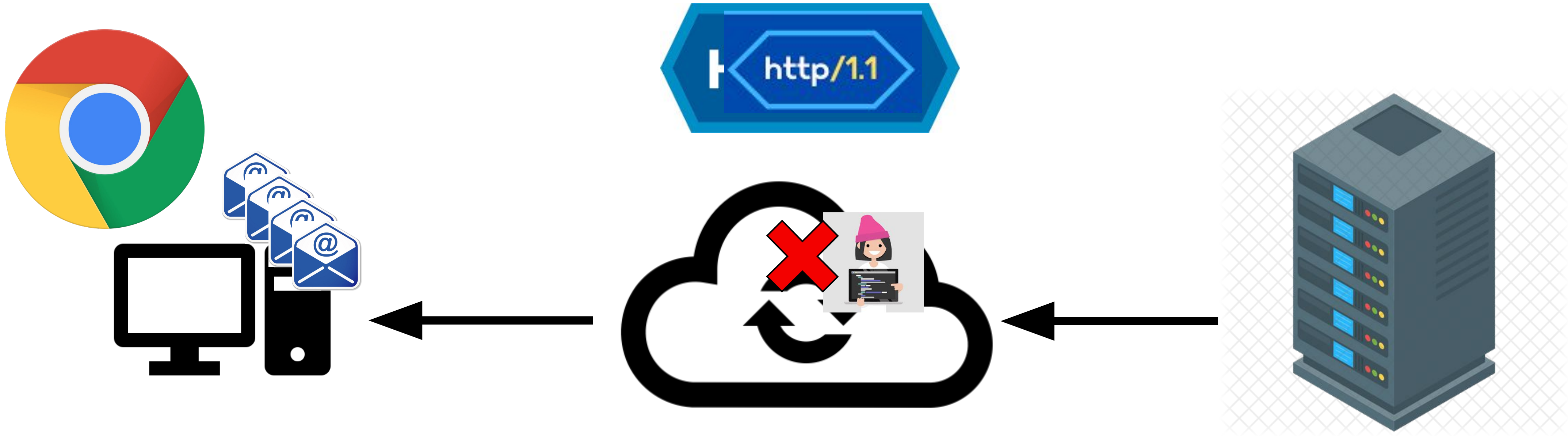


only drop packets selectively - server will think that it is network condition

if drop all the packets server will know its a dos attack

Attack III: HTTP/2 Protocol Degradation Attack

HTTP/2 allows web resource multiplexing for (1) Performance, and (2) to prevent packet size-based ETA.



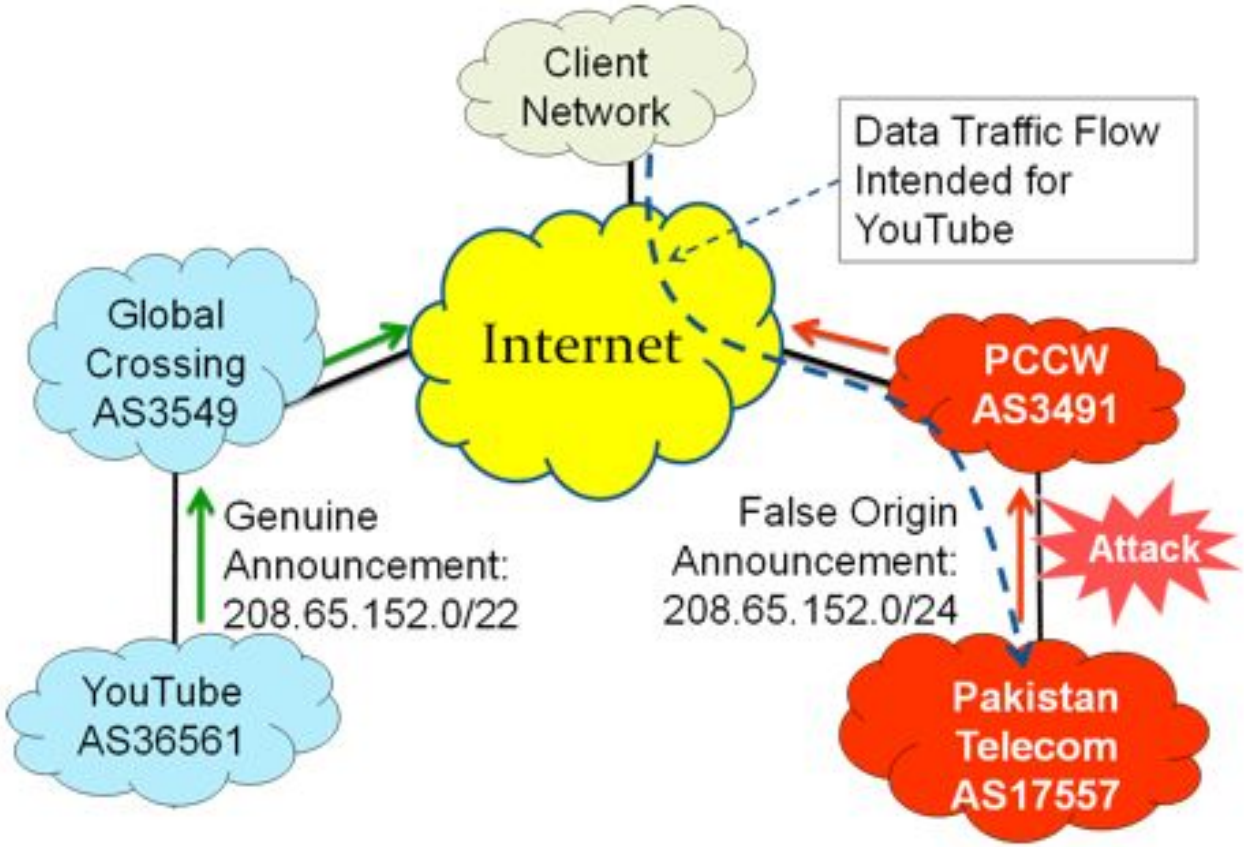
User Device

Internet

Server

Attack IV: BGP Route Hijacking Attack (Basics)

Attack IV: BGP Route Hijacking Attack


Client Network
Data Traffic Flow Intended for YouTube
Global Crossing AS3549
Internet
PCCW AS3491
Genuine Announcement: 208.65.152.0/22
False Origin Announcement: 208.65.152.0/24
Attack
YouTube AS36561
Pakistan Telecom AS17557

Self Learning Topics (in Order of Priority)

Self-Learning Topics

- hping3 tool for generating traffic
- Intrusion Detection System and Snort