OWASP ALGIERS

DDoS Attacks and Mitigation Strategies

Welcome to the official Algiers Chapter of OWASP
(Open Worldwide Application Security Project)

Table Of Contents

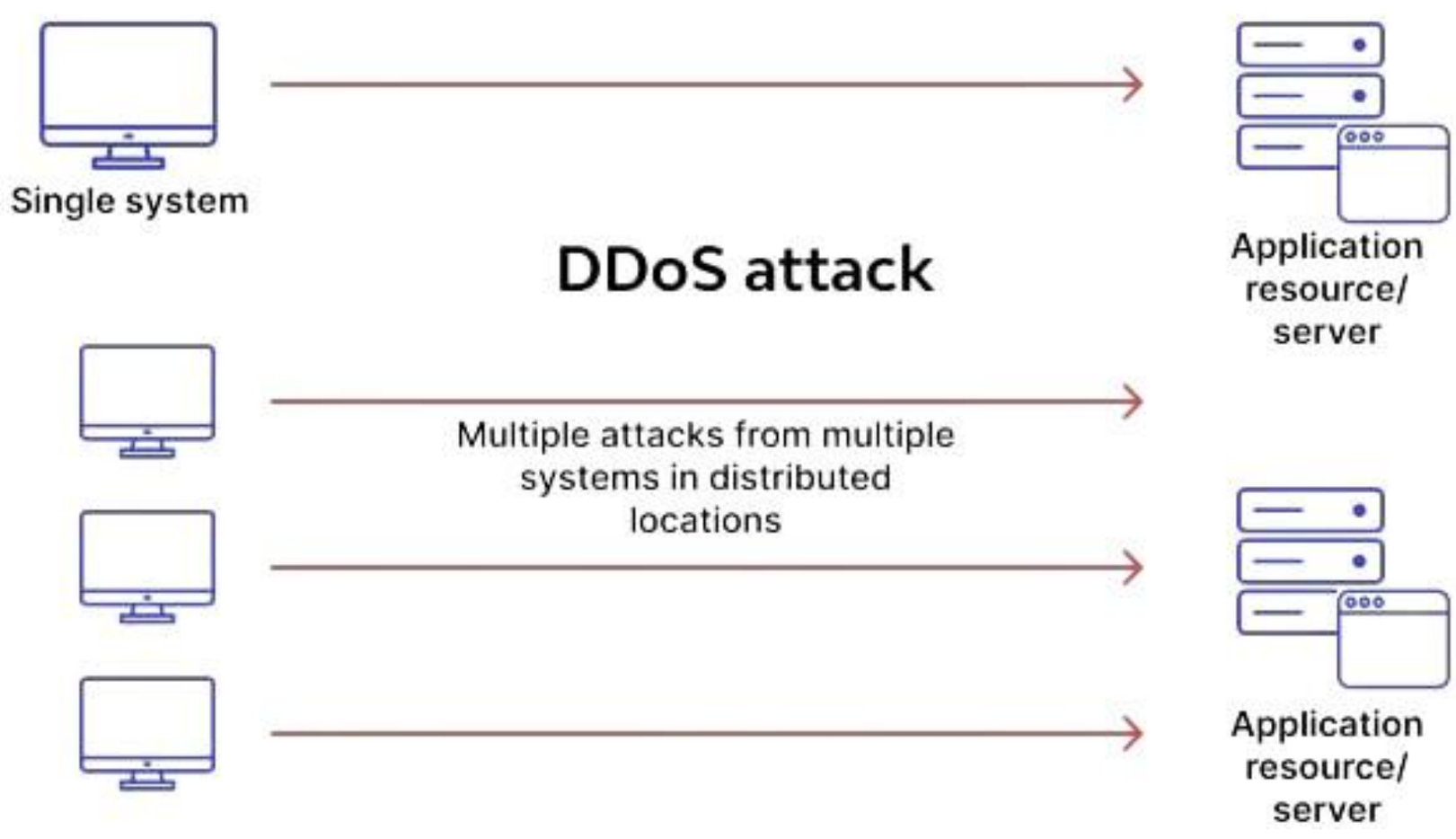
#WHOAMI

- **CyberSecurity Enthusiast**
- **Network Engineer @AGB**
- **Vice President @OWASP Algier Chapter**
- **Board Member @CSA Algeria Chapter**
- **CTF Player, Speaker**

Introduction To DDoS

- **DDoS stands for Distributed Denial of Service.**
- It aims to **overwhelm** a target system with traffic from multiple sources, typically via a botnet.
- The goal is to render services **unavailable** to legitimate users.
- Unlike traditional DoS, DDoS leverages scale and distribution for greater impact.

What is DoS and why it’s effective Anymore?



Impact of DDoS on Business

01

Revenue Loss

Every minute of downtime can result in **losses ranging from thousands to millions of dollars**, depending on the business scale.

02

Brand Damage

Repeated outages erode user trust and tarnish brand reputation. This can impact customer loyalty and market competitiveness.

03

Legal/Regulatory Penalities

Failure to maintain service availability may breach SLAs or regulations. This exposes companies to fines and legal scrutiny.

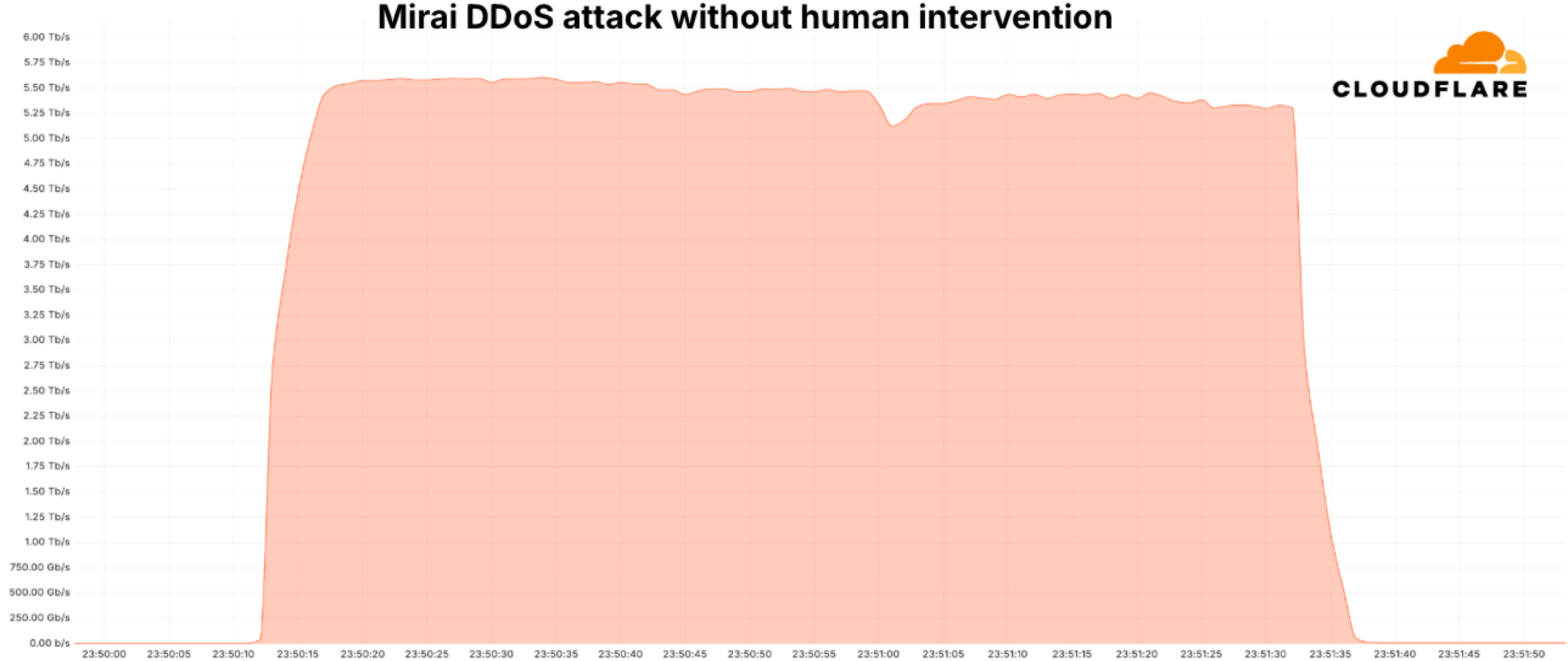
04

Operational Distruption

DDoS attacks can paralyze internal systems and workflows. Employees and services face delays or complete inaccessibility.

Case Studies: Most Impactful DDoS

Target	Volume	Duration	Protocol
Github	1.35 Tbps	20 mins	Memcached
AWS	2.3 Tbps	Days	CLDAP
AZURE	3.47 Tbps	Hours	NTP,CLDAP,DNS
CloudFlare	5.6 Tbps	80s	HTTP
Google	2.54 Tbps	6 Months Campains	*CLDAP, DNS*


Cloudflare's autonomous DDoS defenses mitigate a 5.6 Tbps Mirai DDoS attack without human intervention
CLOUDFLARE
6.00 Tb/s
5.75 Tb/s
5.50 Tb/s
5.25 Tb/s
5.00 Tb/s
4.75 Tb/s
4.50 Tb/s
4.25 Tb/s
4.00 Tb/s
3.75 Tb/s
3.50 Tb/s
3.25 Tb/s
3.00 Tb/s
2.75 Tb/s
2.50 Tb/s
2.25 Tb/s
2.00 Tb/s
1.75 Tb/s
1.50 Tb/s
1.25 Tb/s
1.00 Tb/s
750.00 Gb/s
500.00 Gb/s
250.00 Gb/s
0.00 b/s
23:50:00
23:50:05
23:50:10
23:50:15
23:50:20
23:50:25
23:50:30
23:50:35
23:50:40
23:50:45
23:50:50
23:50:55
23:51:00
23:51:05
23:51:10
23:51:15
23:51:20
23:51:25
23:51:30
23:51:35
23:51:40
23:51:45
23:51:50

Types of DDoS Attacks

01

Volumetric Attacks

- Consume all available network bandwidth
- Send high volumes of traffic or request data to the target
- Amplification Factor: Can reach up to 50x–100x or more.

02

Protocols Attacks

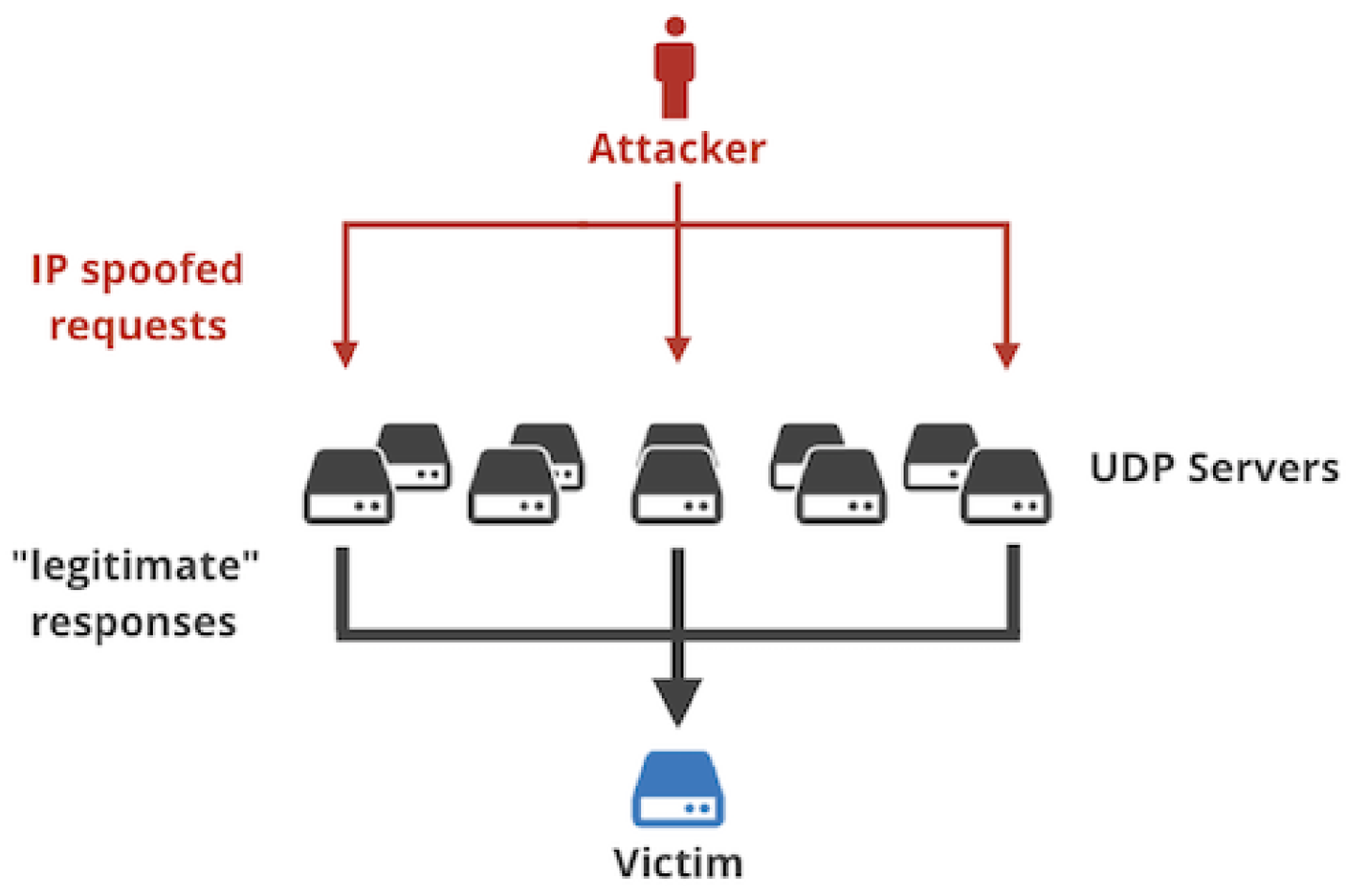
- Exhaust server resources or intermediate devices
- Exploit vulnerabilities in network protocols at layers 3 and 4.
- **E.g:** Exploits TCP handshake by sending many incomplete SYN requests.

03

Application Layer Attacks

- Crash or overload the application/service itself.
- Send seemingly legitimate HTTP/S requests at high volume or frequency.
- Low traffic volume can still cause downtime

DDoS Attack Techniques: Amplification and Reflection



The Solutions

Application-Level Controls:

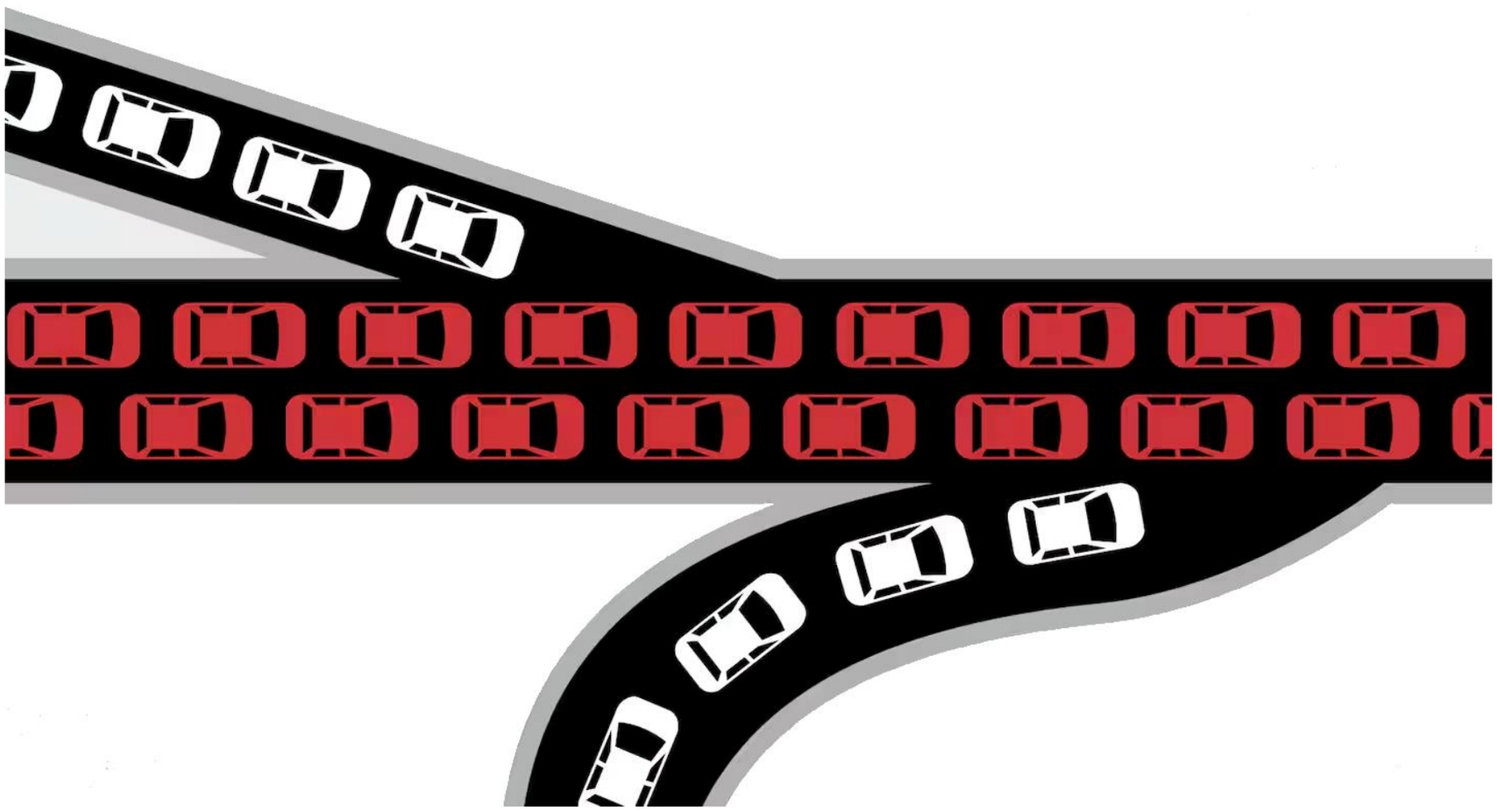
- ✓ **Web Application Firewall (WAF):** Blocks malicious HTTP requests, applies rate limits, uses CAPTCHA
- ✓ **Rate Limiting:** Restricts the number of requests per IP; must be combined with app-level and WAF for effectiveness
- ✓ **Timeouts & Connection Limits:** Reduce idle timeouts, limit connections per IP
- ✓ **Application Logging:** Monitor logs for unusual or malformed access patterns

Protocol-Level Controls:

- ✓ **SYN Flood Protection via Firewalls:** Enable SYN cookies, drop suspicious connections
- ✓ **Ingress Filtering:** Discard malformed or non-compliant packets

Volumetric Protection Controls:

- ✓ Volumetric Attack Could be mitigated only on your **Next-Hop Level**



OWASP ALGIERS

THANK YOU FOR Listening!!!

CONTACT US:

Resources!!

- GitHub DDoS Attack – 2018
- AWS DDoS Attack – 2020
- Google DDoS Attack – 2017
- Azure DDoS Attack – 2021
- Cloudflare DDoS Threat Report – 2024 Q4


OWASP
ALGIERS