SYN Flood

Introducción a los Sistemas Distribuidos (75.43)

Universidad de Buenos Aires, Facultad de Ingeniería

Octubre, 2021

SYN Flood

- ¿Qué es?
- ¿Se usa?
- ¿Cómo puede impactarle a los servidores de Mark Zuckerberg?

DoS

Service Unavailable

HTTP Error 503. The service is unavailable.

El atacante busca hacer que un determinado servicio (por lo general en internet) no esté disponible para un usuario legítimo.

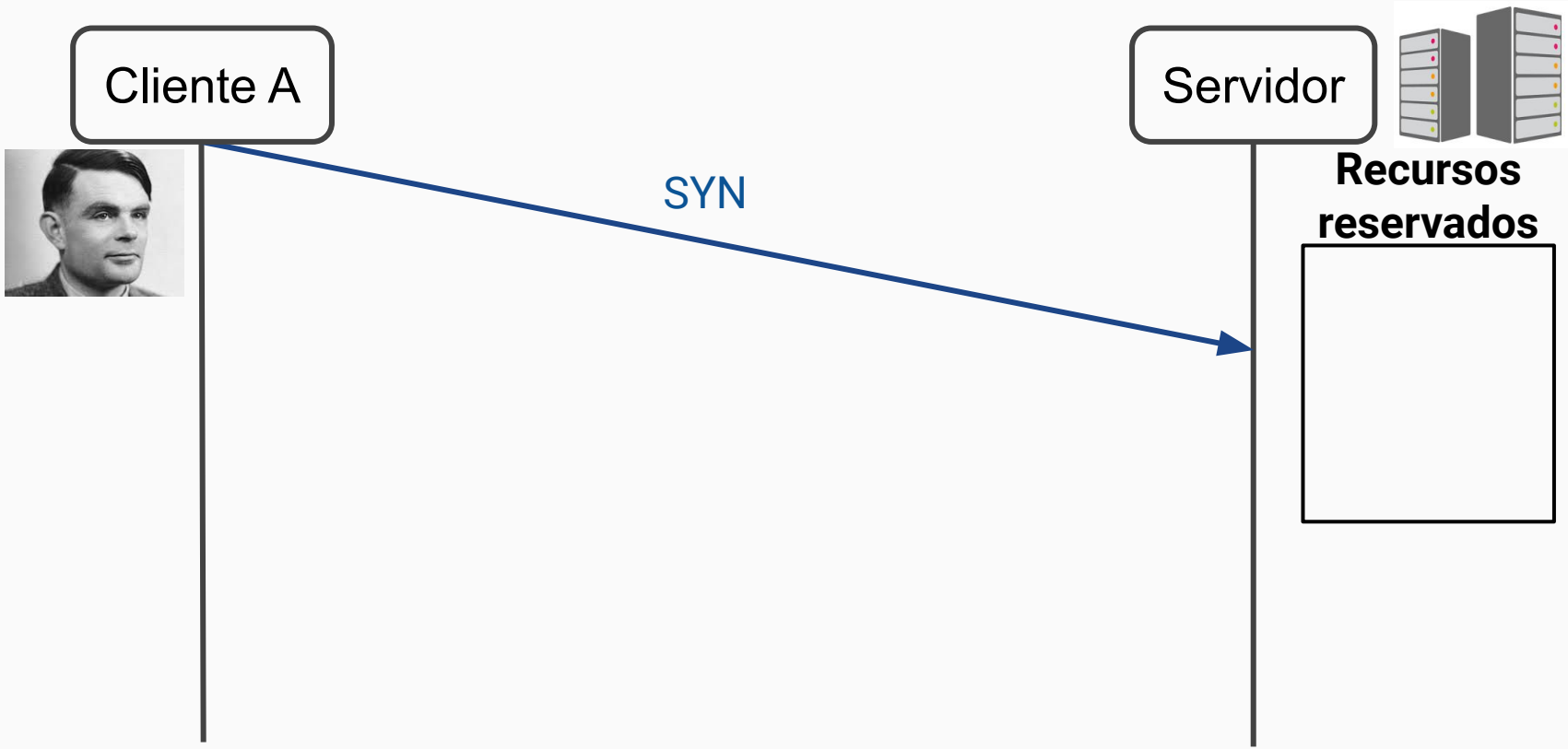
SYN Flood

- Es un tipo de ataque de denegación de servicio (DDoS) que busca [illegible] para el tráfico legí[illegible]ursos disponible[illegible]

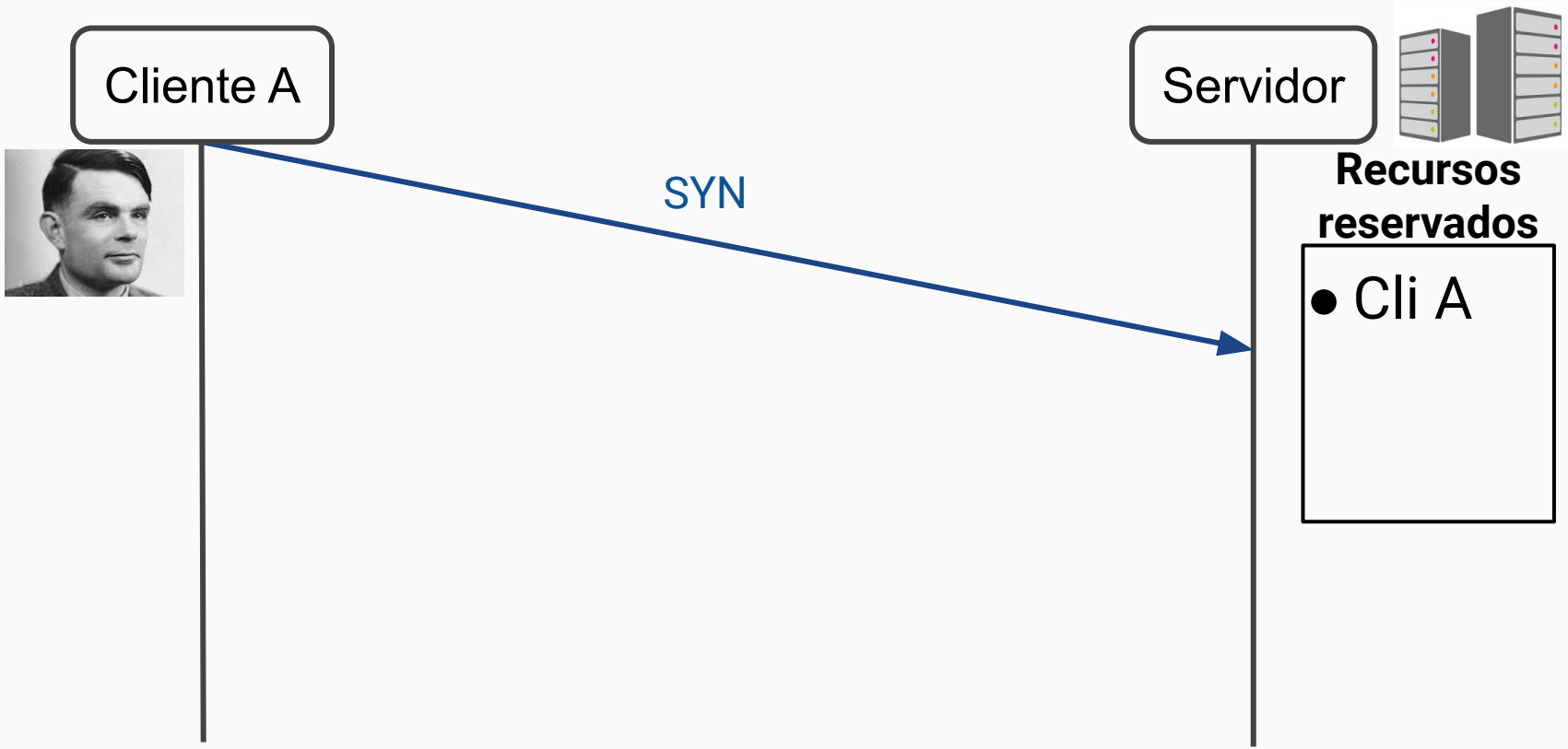
¿Qué **recursos** reserva el servidor?

¿Cuándo reserva **recursos**?

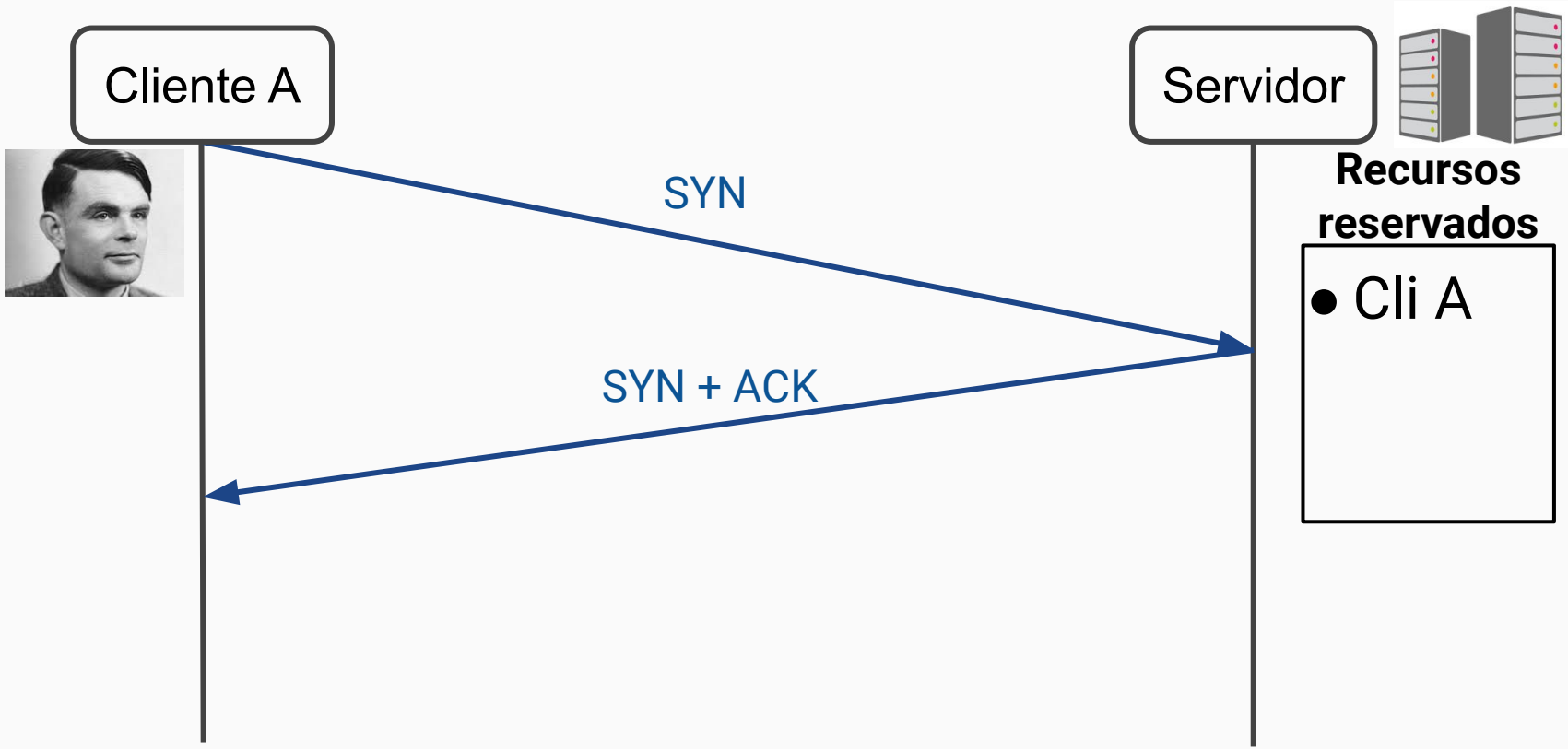
Three way handshake ordinario



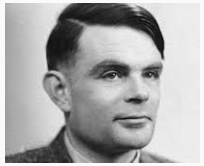
Three way handshake ordinario



Three way handshake ordinario



Three way handshake ordinario



Cliente A

Servidor

SYN

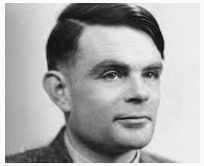
SYN + ACK

Recursos reservados

- Cli A

Reserva recursos cuando envía SYN + ACK

Three way handshake ordinario



Cliente A

Servidor

SYN

SYN + ACK

ACK

Recursos reservados

- Cli A

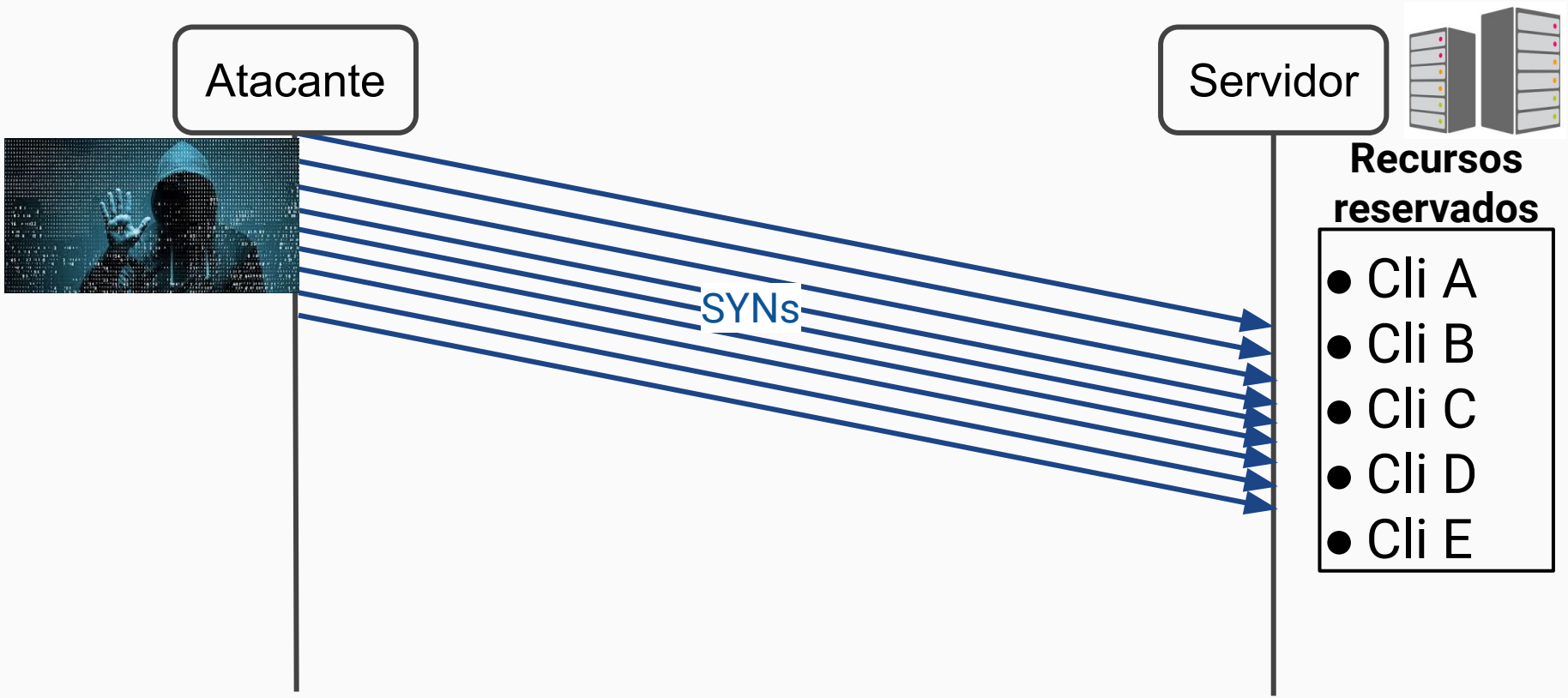
Se inicia la conexión

SYN Flood

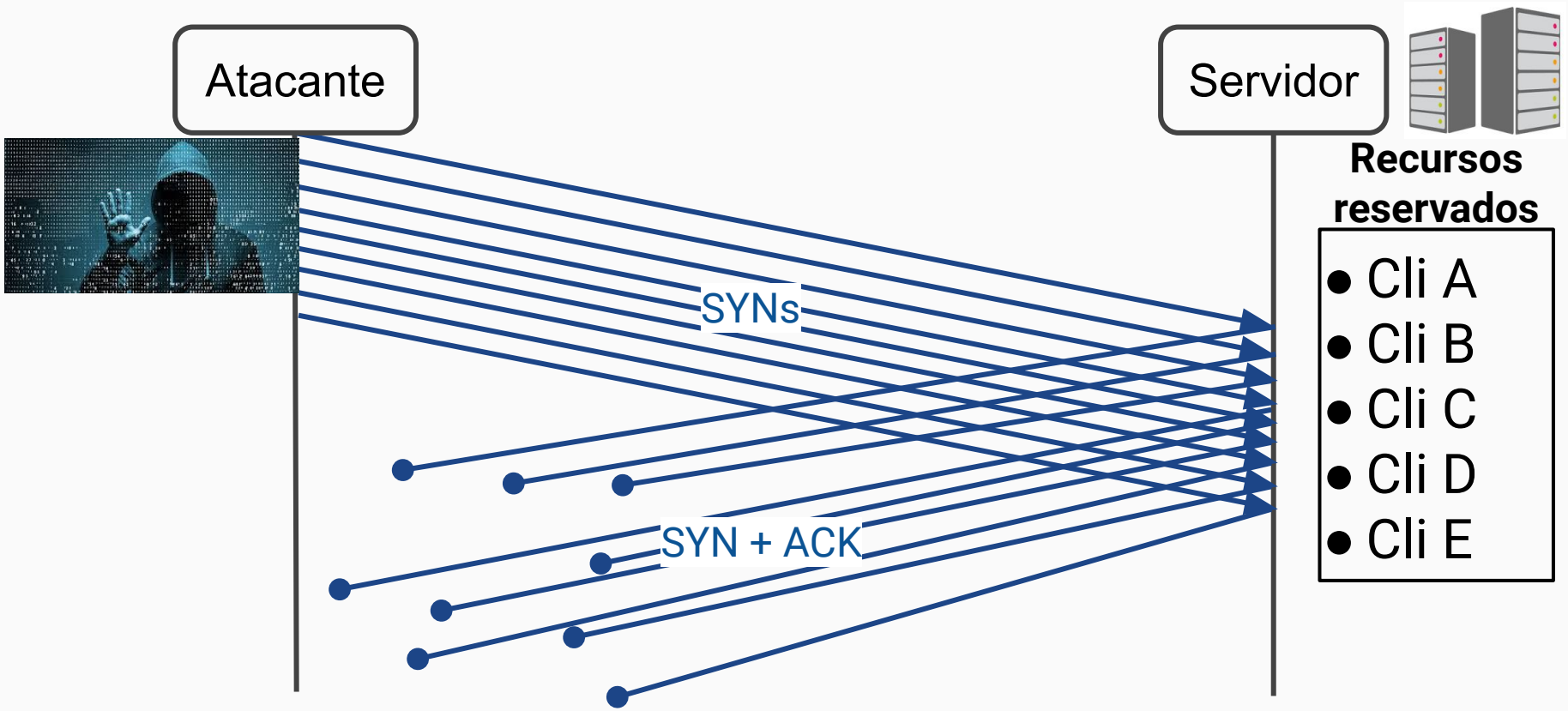
El servidor **reserva recursos** cada vez que recibe un SYN **¿Por qué?**

- Tiene que **guardar info** sobre la conexión de cada cliente que le envió un *SYN*

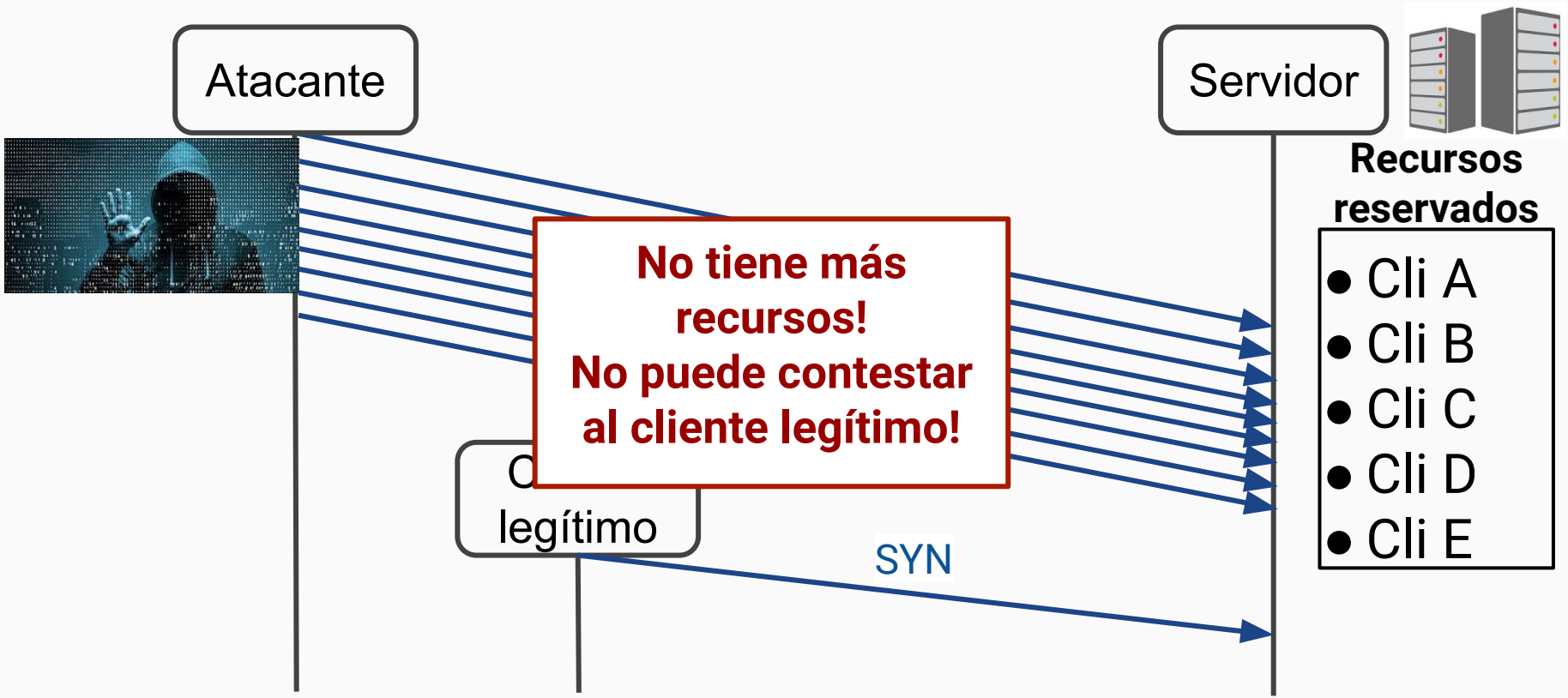
SYN Flood en acción



SYN Flood en acción



SYN Flood en acción



SYN Flood

- Posibles maneras:
  1. Ataque directo
  2. Ataque con paquetes falsificados
  3. Ataque distribuido (DDoS)

SYN Flood: Ataque directo

El atacante:

- No oculta IP
- Sólo utili spositivo de origen

¿Soluciones?

SYN Flood: Ataque con paquetes falsificados

El atacante:

- Falsifica la dirección IP de cada paquete SYN que se envía al servidor destino

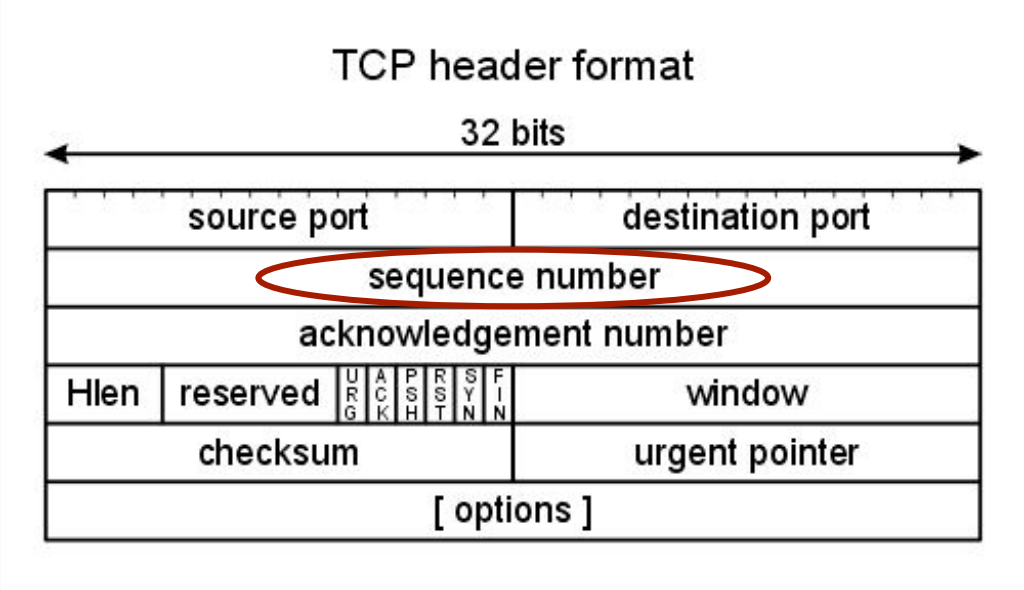
SYN Flood: Ataque distribuido

El atacante:

- Utiliza una red de bots u otras computadoras para realizar el ataque.

SYN Flood: SYN Cookies

- Las ***SYN cookies*** son una forma en particular de elegir los seq numbers



SYN Flood: SYN Cookies

Para construir la SYN Cookie necesitamos de los siguientes elementos:

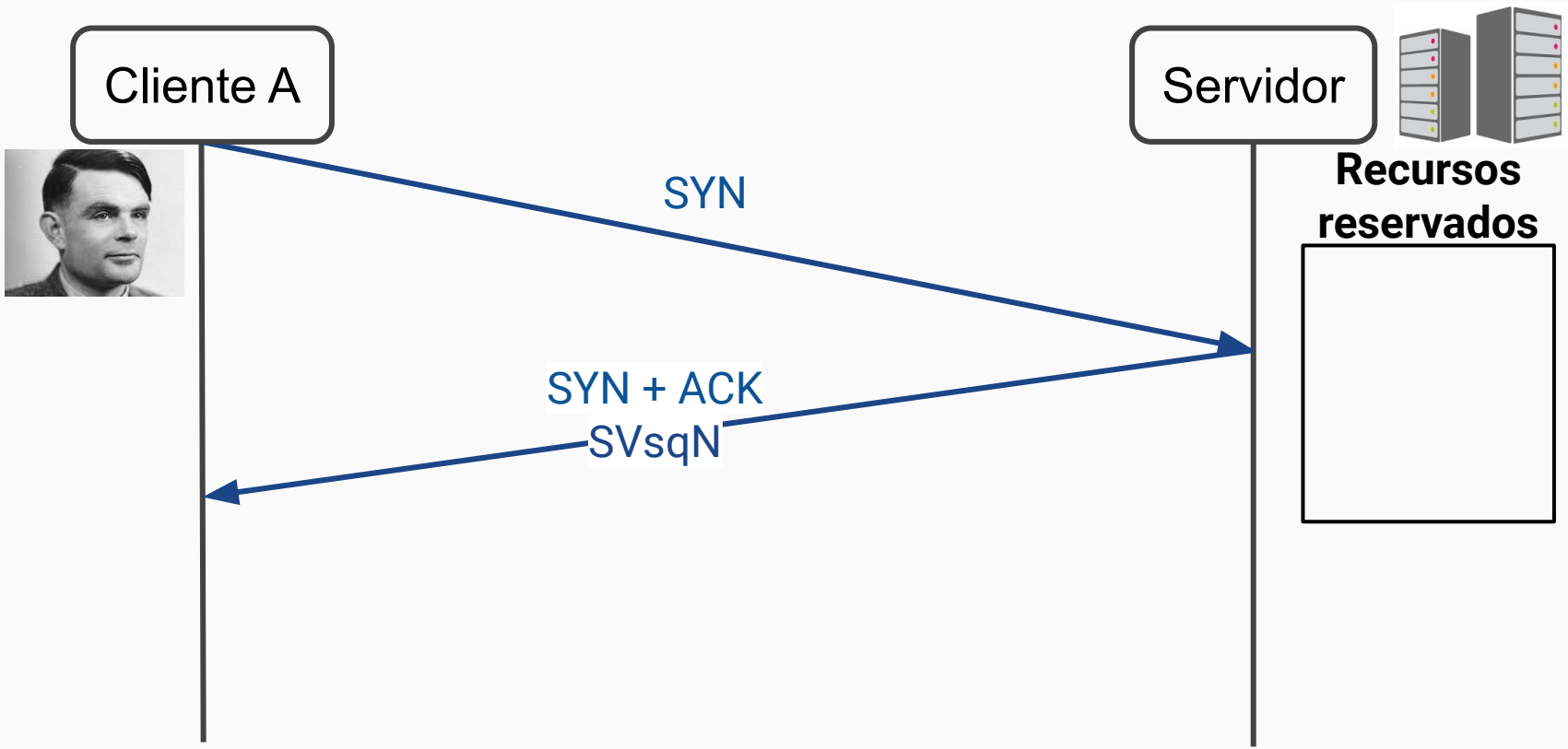
- t = Un Timestamp
- m = Encoded MSS
- s = F(ip_serv, num_puerto_serv, ip_cliente, num_puerto_cliente, t)
  - F es una función secreta de cifrado

SYN Flood: SYN Cookies

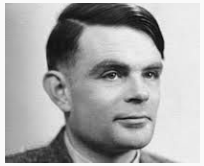
El número de secuencia TCP inicial en SYN Cookie, se calcula como sigue:

- Primeros 5 bits: t mod 32
- Próximos 3 bits: un valor codificado representando m
- Finales 24 bits: s

SYN Cookies en acción



SYN Cookies en acción



Cliente A

Servidor

SYN

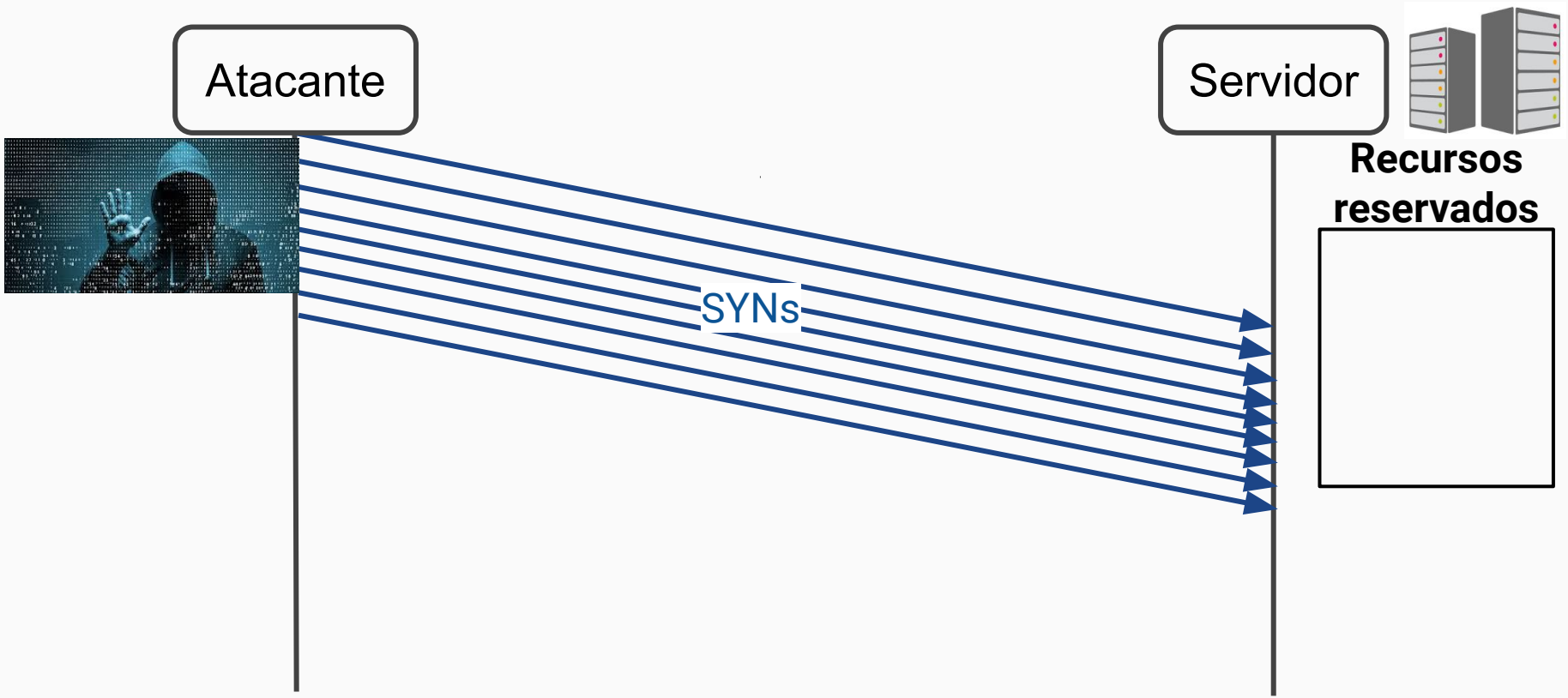
Hace f para el cliente y le suma 1

ACK number = SVsqN + 1

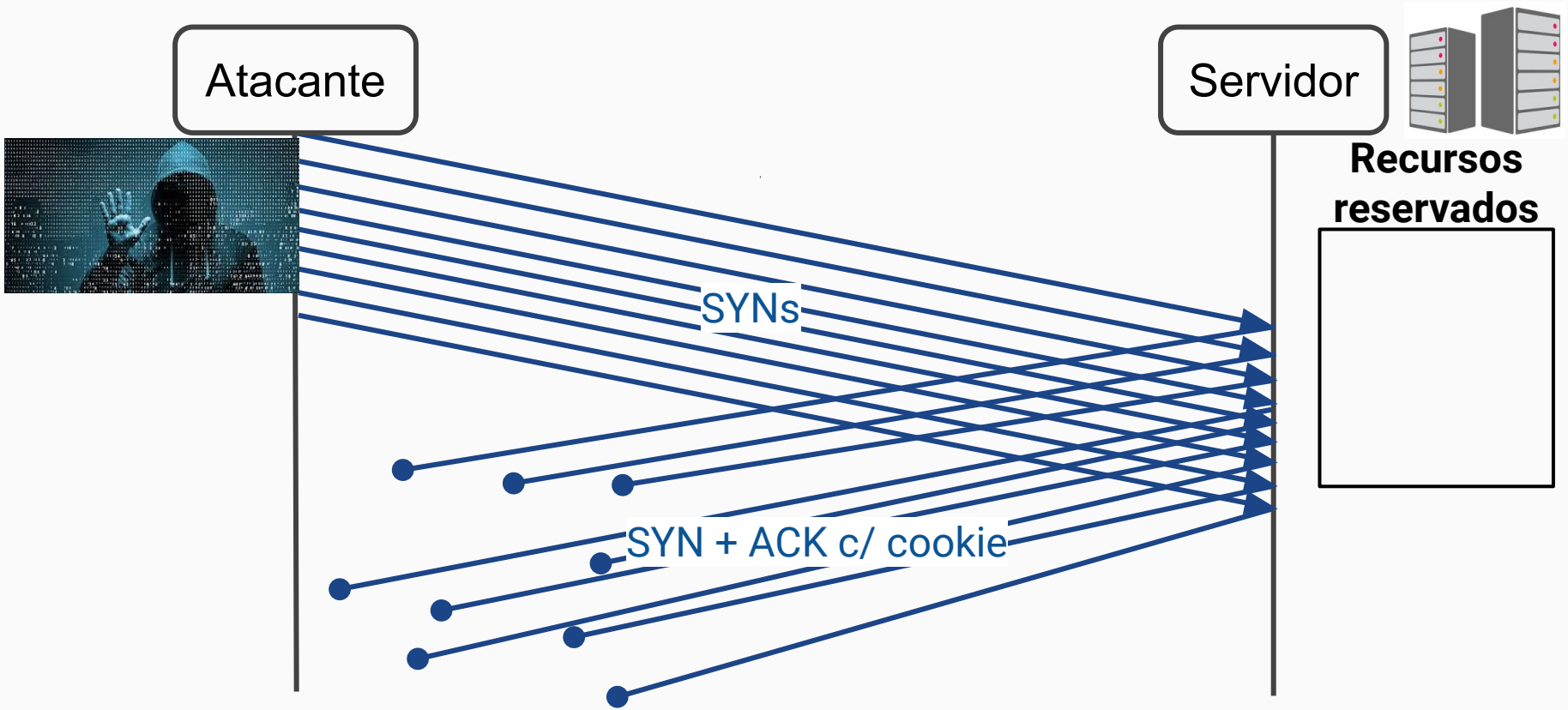
Recursos reservados

- Cli A (se que me contacto antes por el Ns)

¿Por qué funcionan las SYN Cookies?



¿Por qué funcionan las SYN Cookies?



¿Por qué funcionan las SYN Cookies?

Atacante

¿No contesta?

Servidor

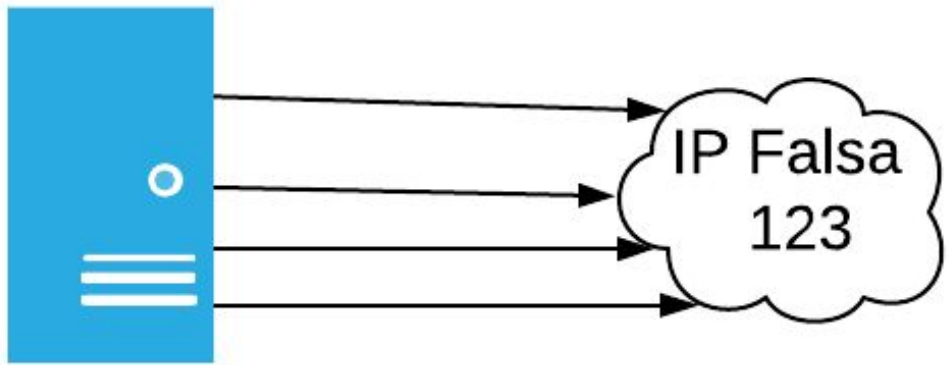
Recursos reservados

SYNs

SYN + ACK c/ cookie

IP Spoofing

- El servidor contesta a esas ips falsas (que no responden)

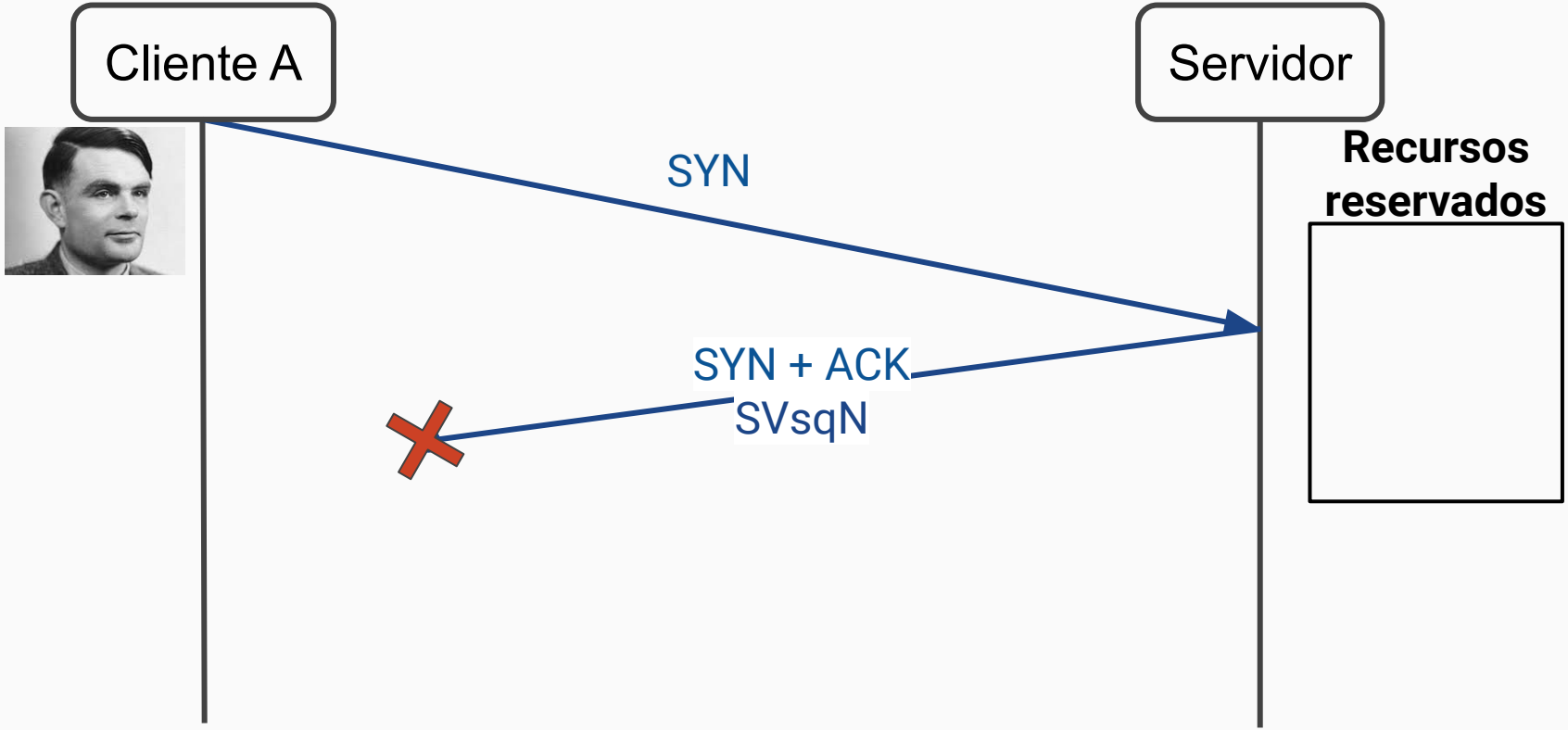


- **Si el atacante quiere contestar, debe exponer su IP**

SYN Cookies: Desventajas

- Se descarta el paquete SYN del cliente, con todas sus opciones (incl. *wnds*)
- El MSS en la *cookie* se guarda con 3 bits -> sólo se pueden guardar 8 valores distintos

SYN Cookies: Desventajas



SYN Cookies: Desventajas

- El cliente quedará esperando suponiendo que la conexión ya se estableció y el servidor no tiene nada para mandar
  - El servidor **no puede reenviar el SYN+ACK** ya que no guardo ningún dato, ni arranco ningún timer.

SYN Cookies: Otras medidas

- Otras medidas listadas en la RFC 4987
  - Filtering
  - Increasing Backlog
  - Reducing SYN-RECEIVED Timer
  - Recycling the Oldest Half-Open
  - TCP SYN Cache
  - Hybrid Approaches
  - Firewalls and Proxies