ROSE-HULMAN
INSTITUTE OF TECHNOLOGY

CSSE 490
Network Security

Day 18: More TCP

Pushing the Envelop

- What is the main objective in a SYN flood attack?

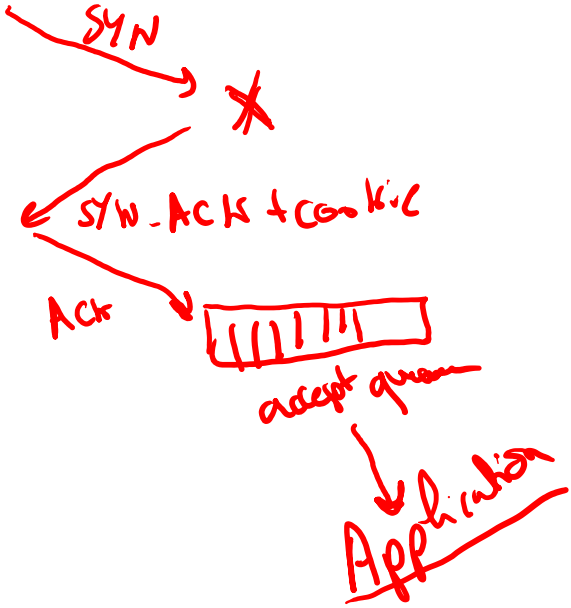
  Fill up the listen } Overwhelm the state at the server } ✓

- Why do SYN cookies work in this case?

  Don't need a queue anymore.

- What could be the next logical target?

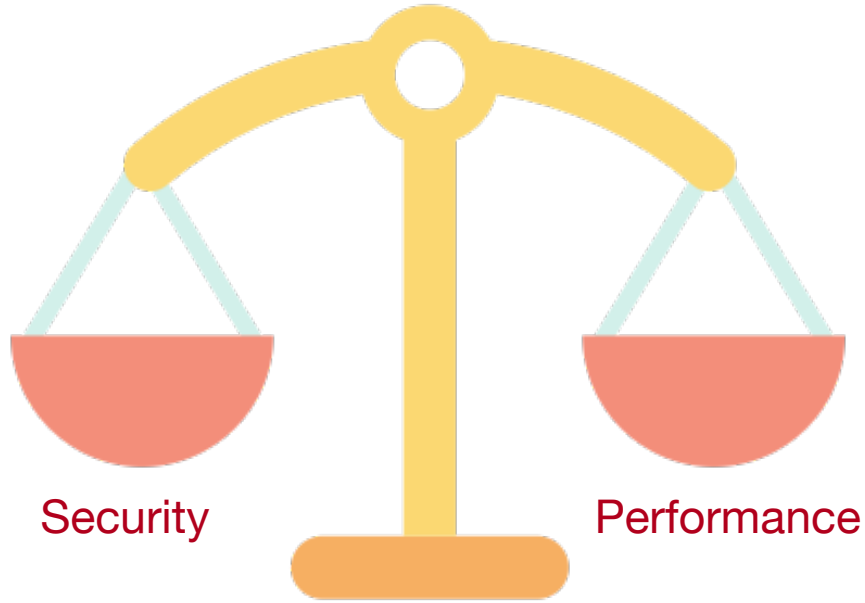
  Accept queue



Security Tradeoff

Security advantage	Performance penalty
Cookie authentication	cookie size

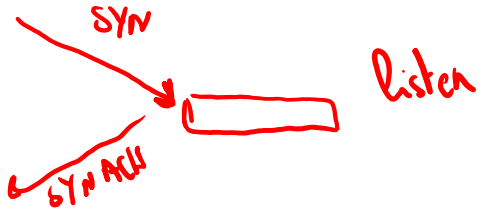
- The server must keep accepting new connections.
- There is thus a tradeoff between **security** and **performance**
- Figuring out the right balance is the job of a good engineer

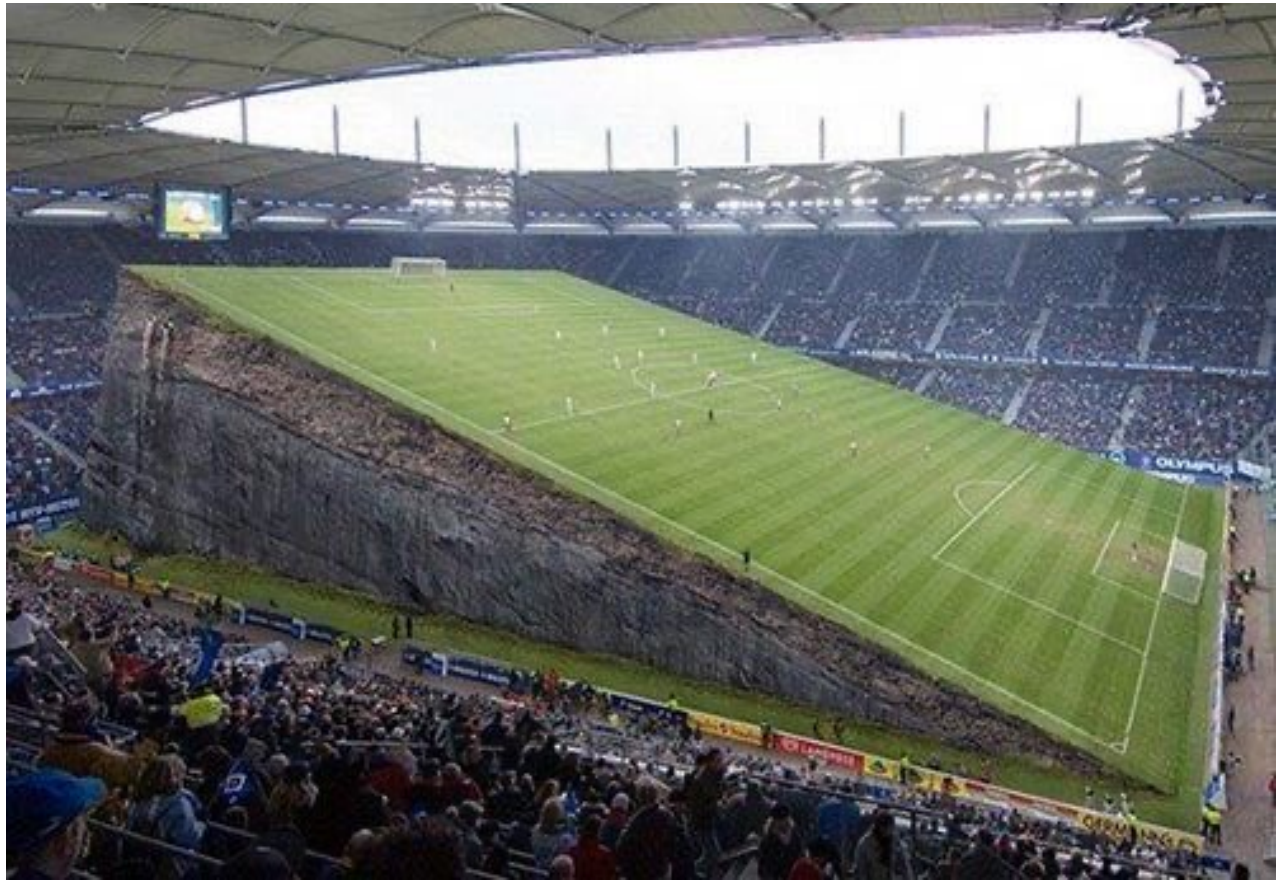


The Main Problem

between the attacker & the defender

- **Unlevel** playing field
- Easy to **spoof** packets
- Easy to send packets
- Server must expand resources **first**





Current Defense Trends

security vs. performance.

performance tradeoff

- Need more defenses that are on-premises
- Involve users in the defense process

Rate limiting

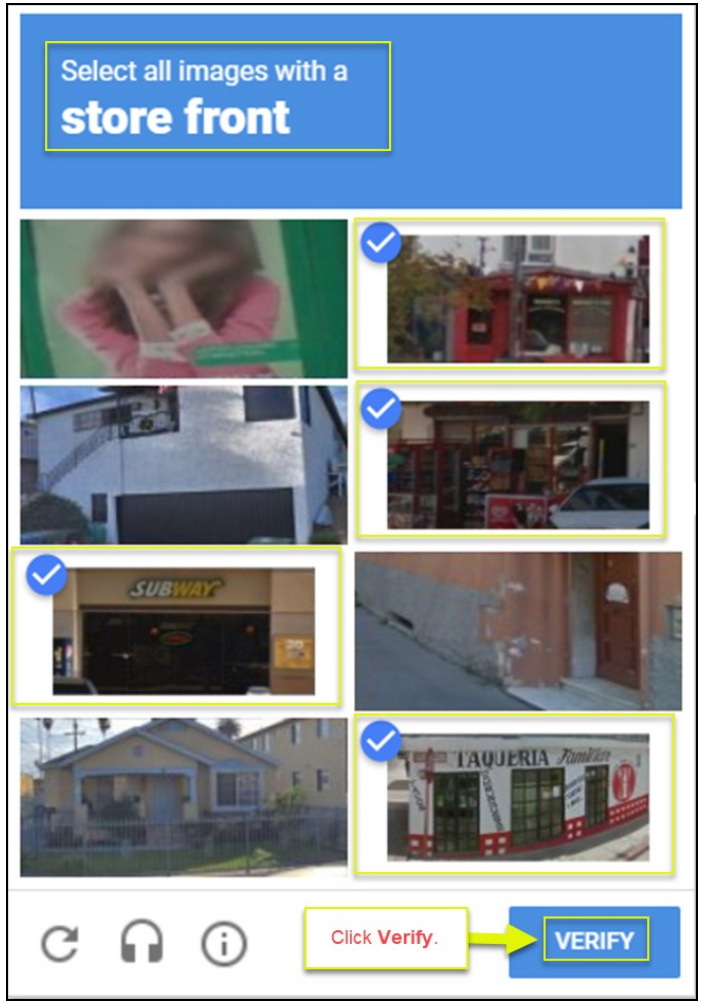
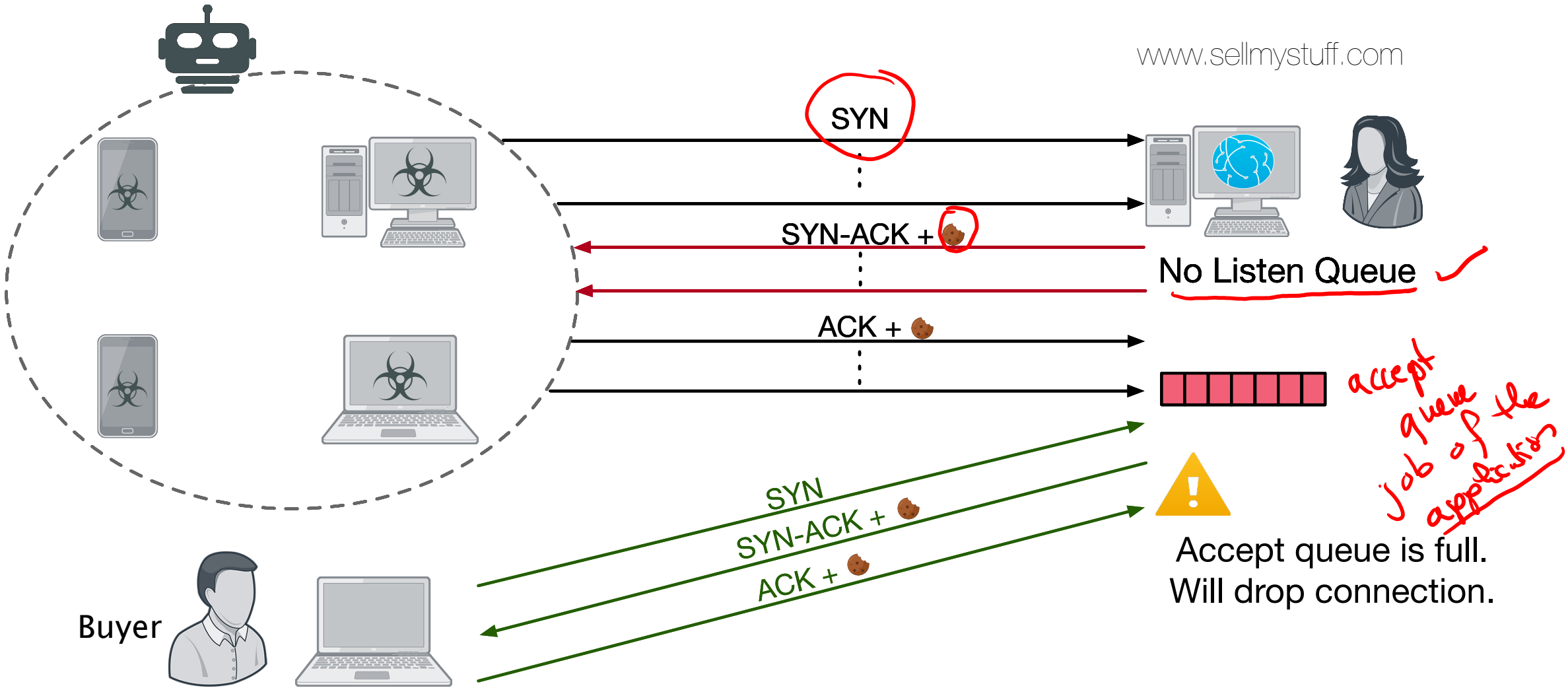


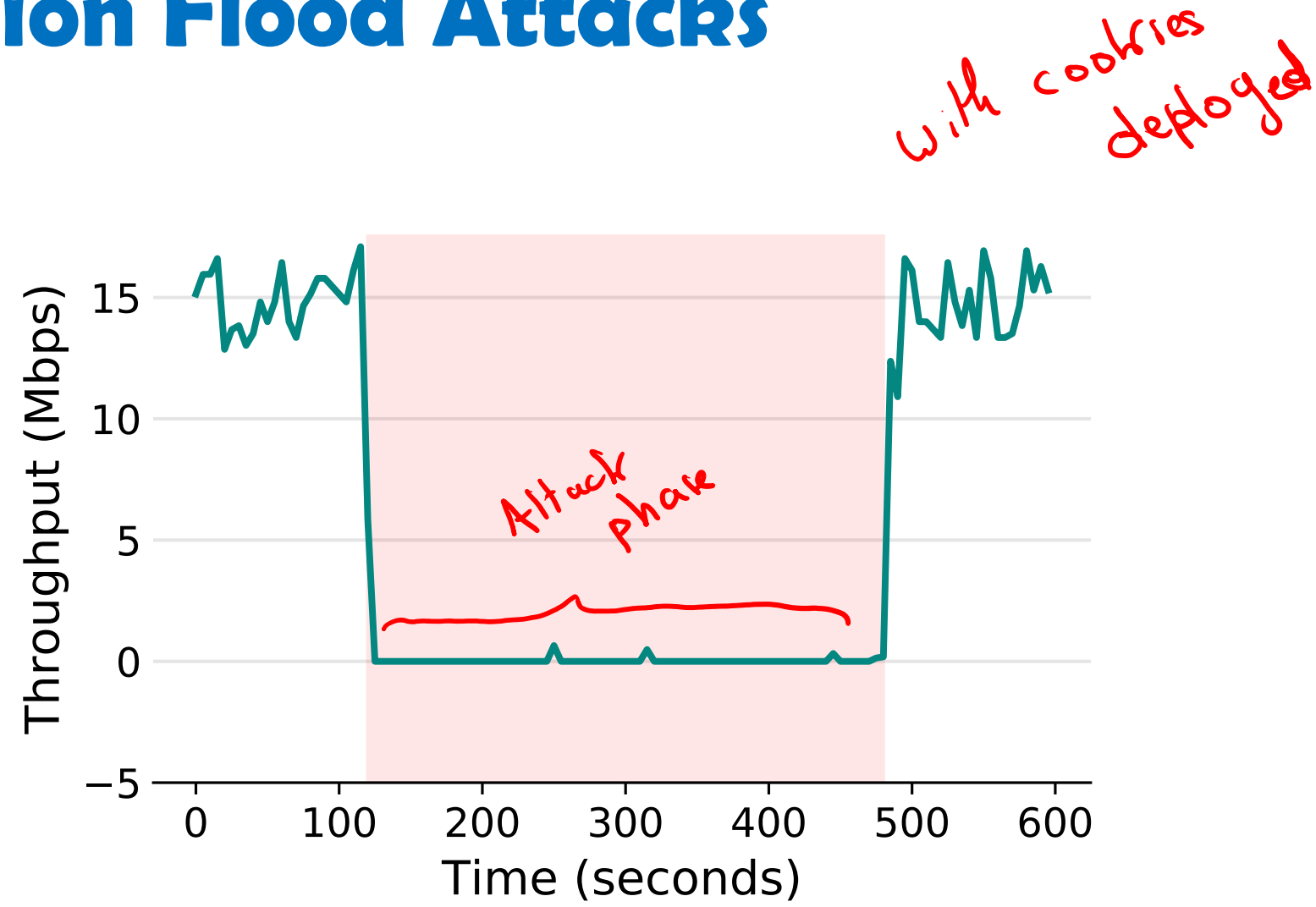
Image on the right: https://support.vagaro.com/hc/article_attachments/360002228693/2.png
Image on the left: https://xkcd.com/233/

Connection Flood Attacks

rate_flood >> rate_accept



Connection Flood Attacks



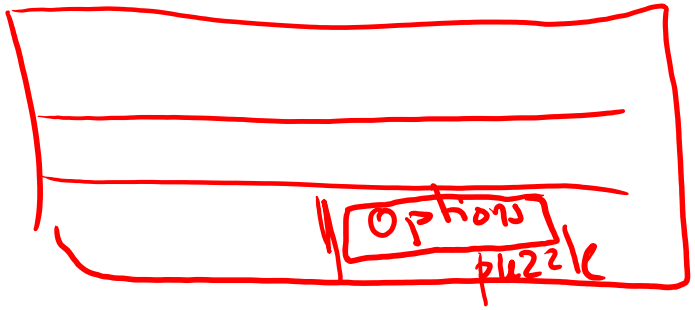
Why do Connection Floods Work?

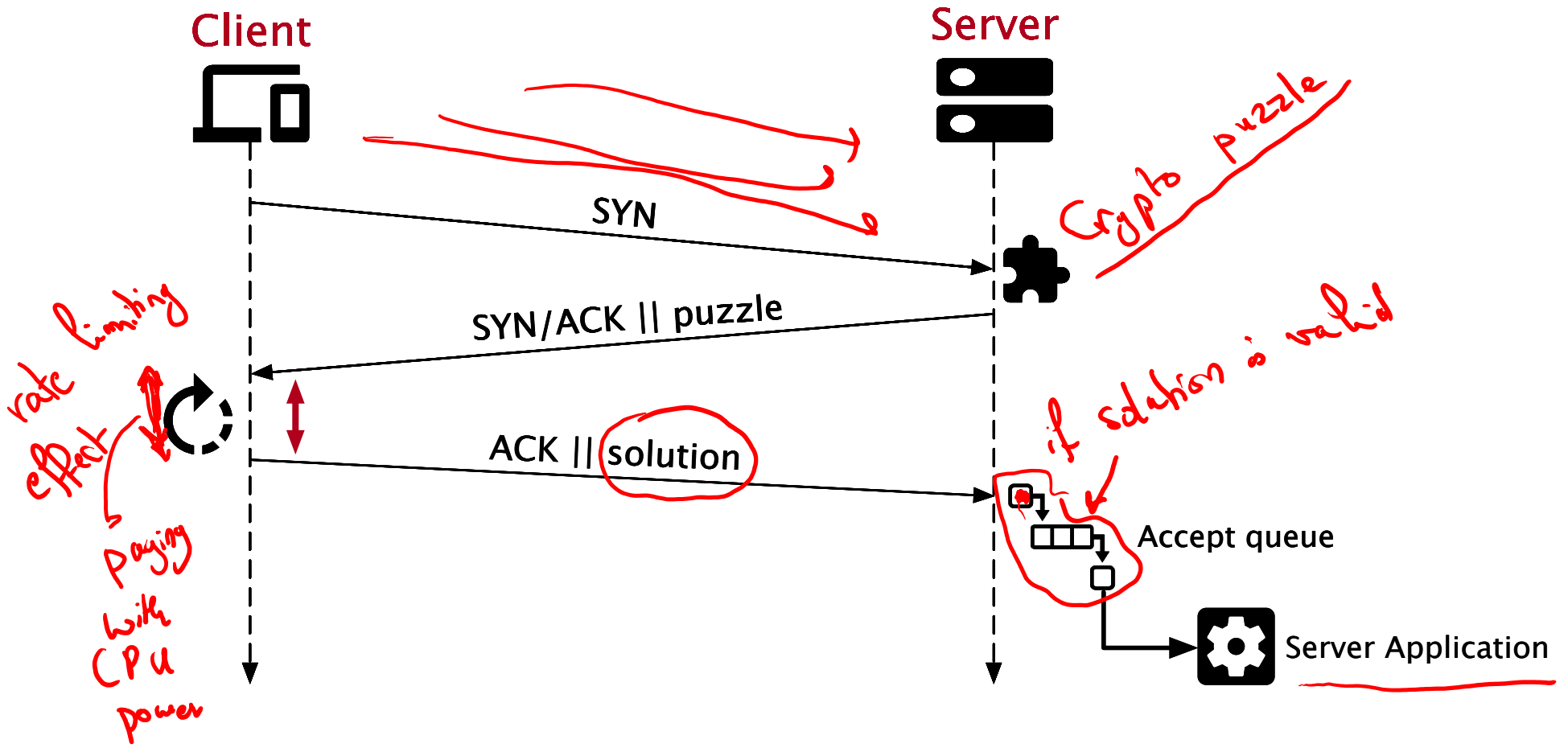
- Compared to a SYN flood, the success of a connection flood is dependent on

- How can

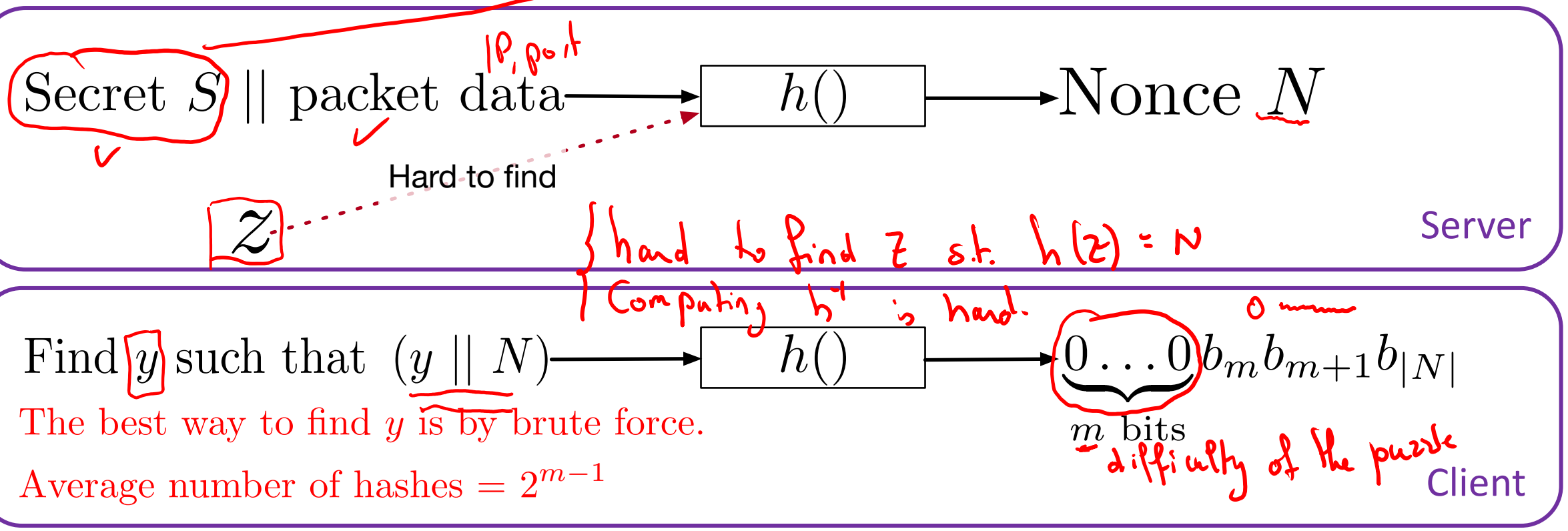
  - They use large botnets, e.g. the Mirai botnet peak at 650k bot devices!

Client Puzzles





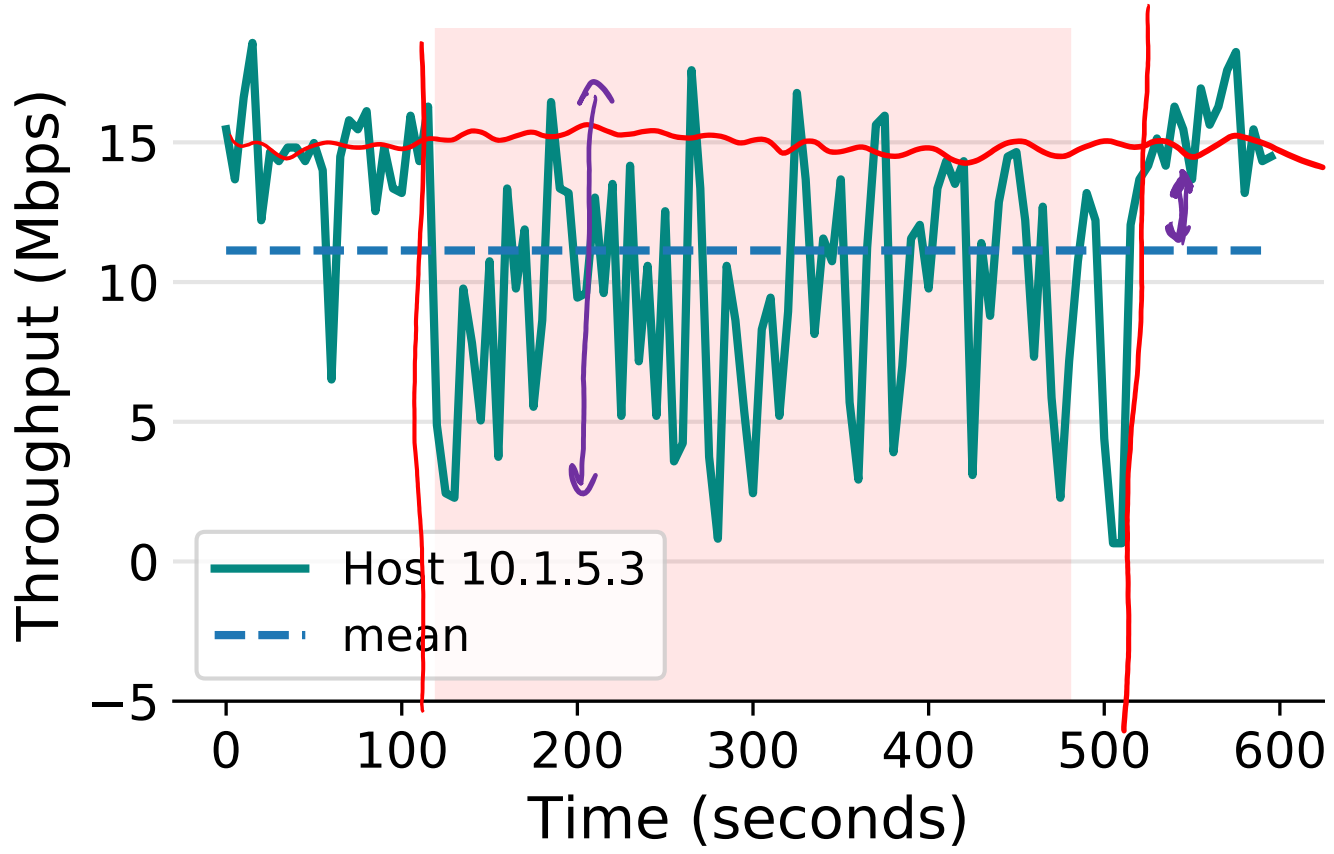
Crypto Puzzles



Regenerate N and verify that $(y \mid\mid N)$ → $h()$ → $\underbrace{0 \ldots 0} b_m b_{m+1} b_{|N|}$ (m bits)

Server

Client Puzzles in Action

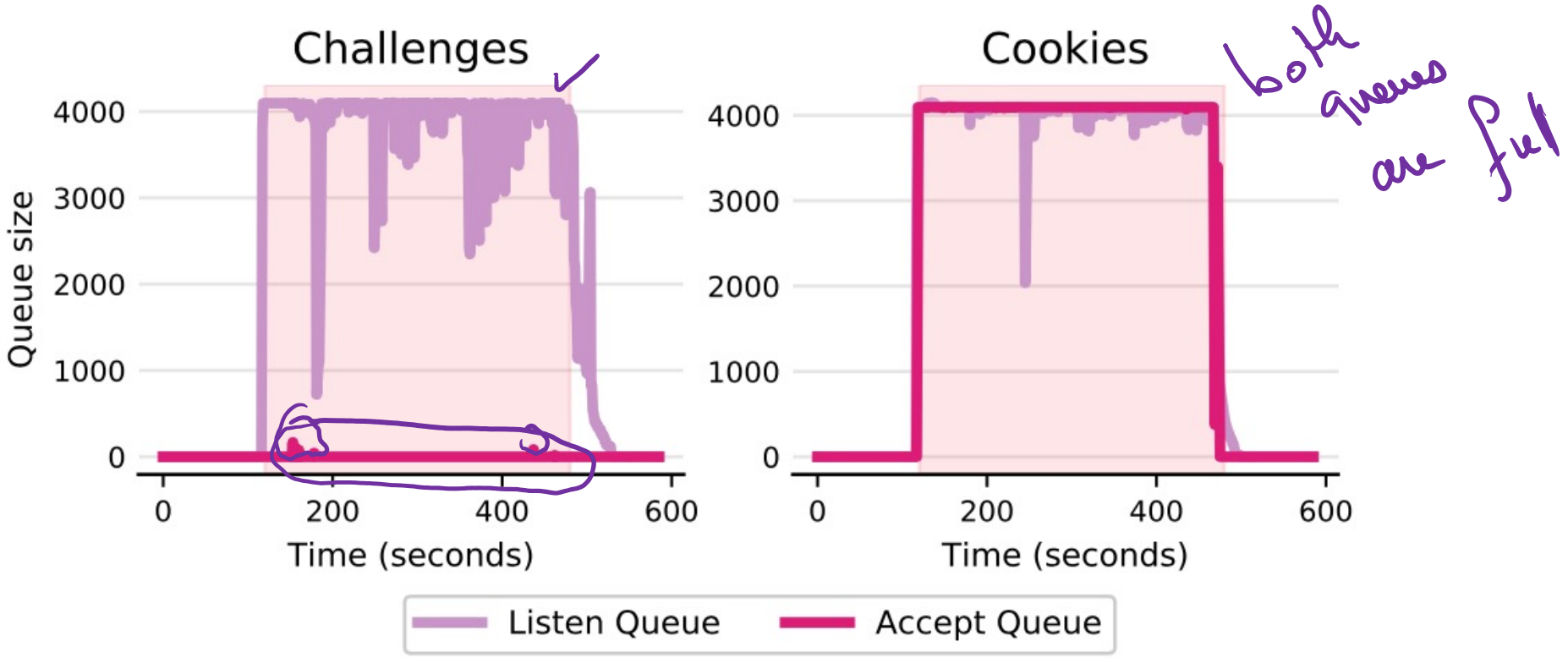


Solving a puzzle takes an undeterministic amount of time

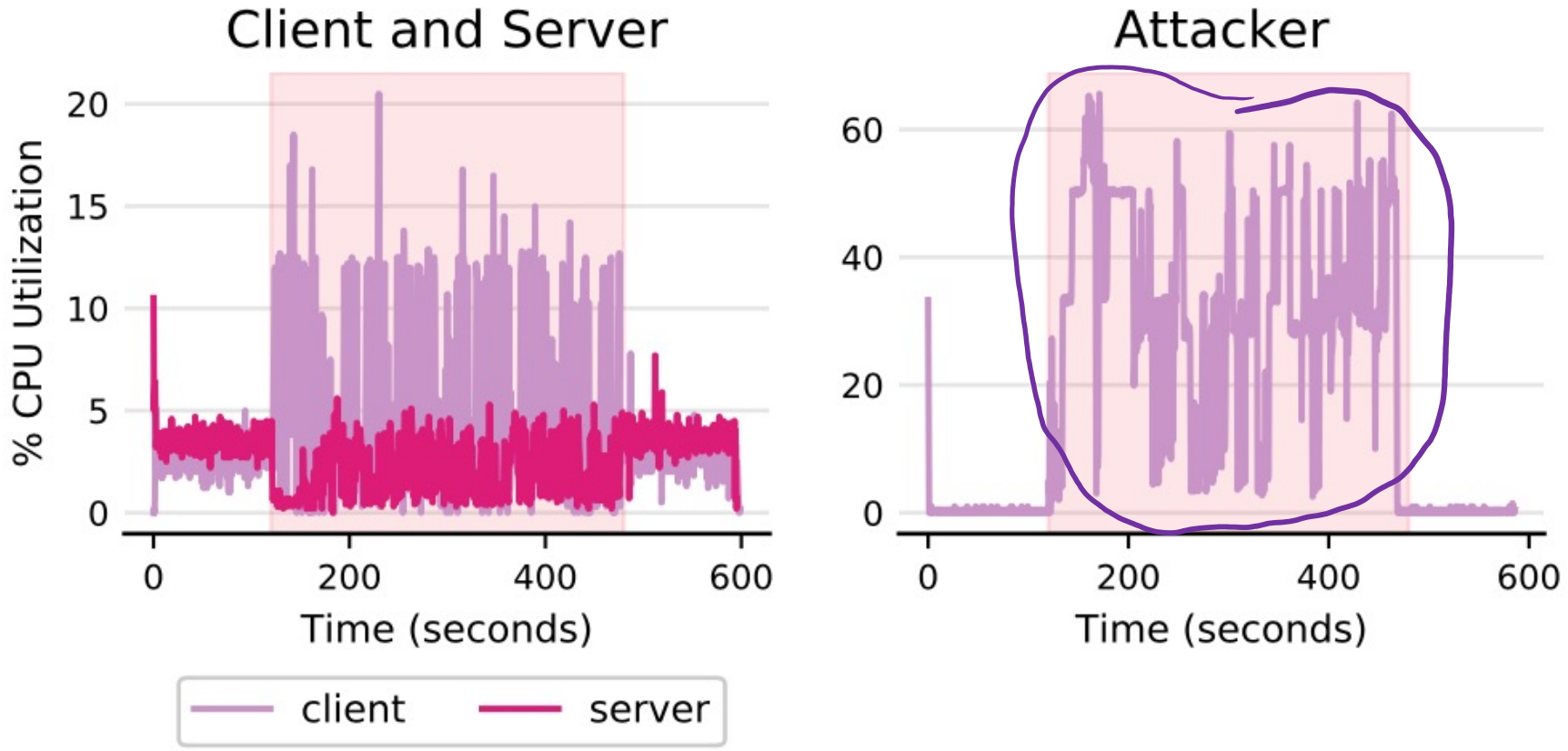
≈

probability distribution over the time to solve

State of the Queues



Impact on CPU Utilization



Next Steps

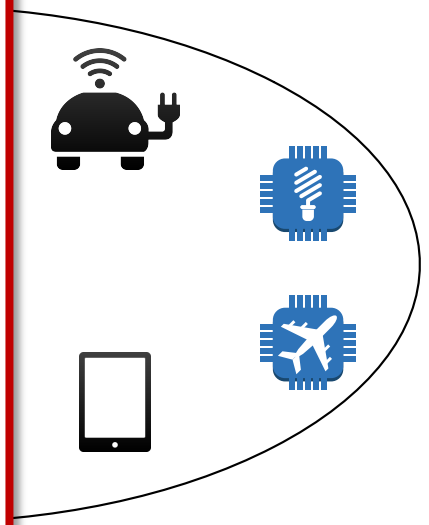
- Heterogeneous set of devices, setting the puzzle difficulty can be very challenging!

Valery Smyslov | Wed, 20 May 2015 06:13:55 -0700

Hi Yaron,

> First, I raised a third concern, which is that allowing the client to decide on the difficulty of the puzzle it is willing to solve adds unneeded complexity. Basically the client doesn't have enough information to make a good decision.

The problem is that the server doesn't have enough information either. Selecting appropriate puzzle difficulty so that weak legitimate clients are not thrown away and, on the other hand, the server could effectively defend against DoS attack looks like the main problem of puzzles.



Recap

- Why is TCP vulnerable to state exhaustion attacks?

Exploit	Targets	By	Mitigated by	Limitation of mitigation technique
Syn Flood	The listen queue	Sending a barrage of SYN packets and not ACKing the SYN-ACK	SYN Cookies	Fails when there is a connection flood.
Connection Flood	The accept queue	Completing a lot of connections faster than the application can process them	Client puzzles	Need to determine a balanced puzzle difficulty, especially with heterogeneous devices.