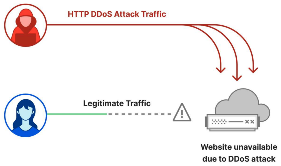
Indiana Statewide
Cybersecurity
Summit 2023

Reintroducing Client Puzzles for DDoS Mitigation

Introducing DDoS:

The Volumetric Distributed Denial of Service Attacks (DDoS) is one of the most common problems in network security. Volumetric DDoS Attacks occur when a server is flooded with so much fake traffic that the server can not serve requests from legitimate clients.

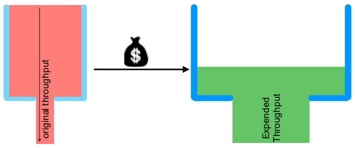
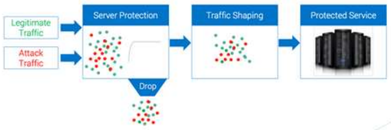


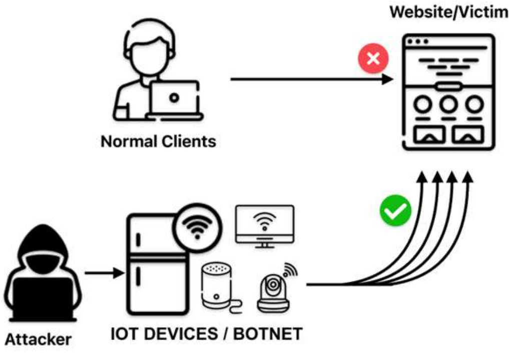
A diagram of how DDoS attacks prevent legitimate internet traffic from being processed

- DDoS attacks can cost a business anywhere from 120,000 – 2 million USD
- Microsoft stopped the largest attack every recorded at 3.47 tbps
- In 2022 Cloudflare mitigated an attack that came from 30,000 different IP address

CLOUDFLARE Microsoft

Current Solutions:

Absorption		
	By absorbing additional traffic just like normal traffic clients should be able to maintain access to the website any not notice any difference	Resource war between attackers and Internet Service Providers Expensive
Filtering		
 Legitimate Traffic Attack Traffic Server Protection Drop Traffic Shaping Protected Service	Filtering techniques sift through all traffic and determine what is a legitimate user and what is not.	resource exhaustion on the filter Filters sometimes drop legitimate traffic
Authorization		
Levelers critics Type the two words: reCAPTCHA stop spam. read books.	Tools like reCAPTCHA or capability tokens can be used to validate if the source of traffic is coming from a legitimate client, or if it is coming from an attack	User typically dislike tools like reCAPTCHA A good attacker can spoof their attack to mask themselves as an authenticated client



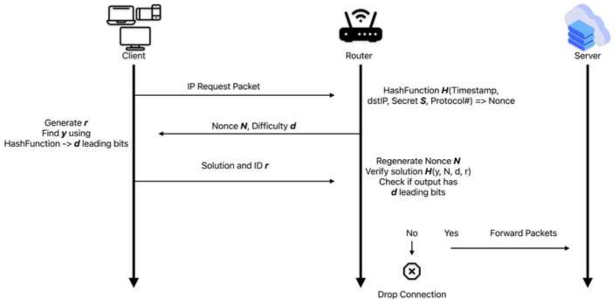
The problem

- DDoS attacks are getting cheaper and cheaper to run
- Current solutions would fail if an attack exceeded the current bandwidth available by mitigation providers.
- The only way to prevent DDoS attacks from impacting victims is to have more resources than attackers can get ahold of

A Solution

- Make attacks more expensive to run by exhausting the attackers' resources
- Improve filtering by collecting more information on the source of the traffic

PUZZLES



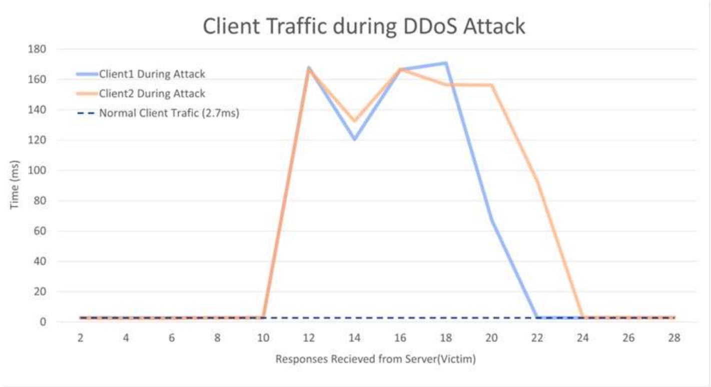
Puzzles are cryptographical challenges imposed on clients trying to access a webserver. Clients can solve puzzles by hashing through a nonce 2^{d-1}times. Therefore, Clients will have to provide more computational work for a larger d.

Strengths:

- All Devices must use computational resources to communicate with a server
- Stateless
- Makes attacks more expensive to run (60% more CPU utilization)
- Computer handles the work not the user

Weakness:

- Fairness issue between devices with strong and weak computational resources
- Computation must happen at kernel level



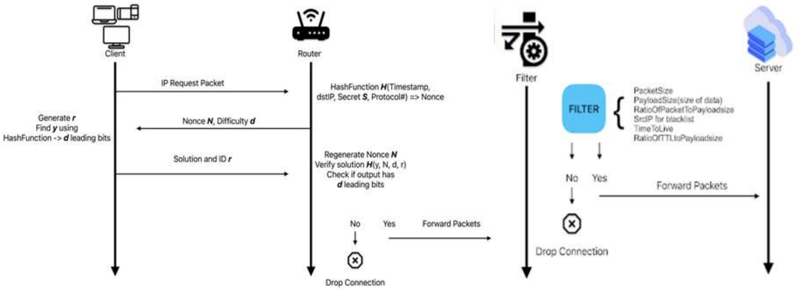
OUR ARGUMENT

Client puzzles with scalable difficult deployed on a flexible network can mitigate the affects of a modern DDoS attack

Where R is the number of resources the server would need to use to fulfill a client's request, we can scale the difficulty (d) like so

$$\boldsymbol{R \uparrow than\ d \uparrow and\ if\ R \downarrow than\ d \downarrow}$$

Implementing this client puzzle protocol system is even easier today with a cloud architecture using software like intel's DPDK that runs applications at kernel level



ROSE-HULMAN

Mohammad Noureddine
Assistant Professor of Computer Science and Software Engineering

Theodore Yin
Undergraduate Computer Science Major

Andrew Walkowski
Undergraduate Computer Science Major