DynaShield: A Cost-Effective DDoS Defense Architecture

Shengbao Zheng
Duke University
szheng@cs.duke.edu

Xiaowei Yang
Duke University
xwy@cs.duke.edu

CCS CONCEPTS

• **Security and privacy** → **Denial-of-service attacks**;

KEYWORDS

DDoS, Serverless, On-demand, Cryptocurrency Mining

ACM Reference Format:

Shengbao Zheng and Xiaowei Yang. 2018. DynaShield: A Cost-Effective DDoS Defense Architecture. In *SIGCOMM Posters and Demos '18: ACM SIGCOMM 2018 Conference Posters and Demos, August 20–25, 2018, Budapest, Hungary*, 3 pages. <https://doi.org/10.1145/3234200.3234232>

1 INTRODUCTION

Large-scale Distributed Denial of Service Attack (DDoS) is a formidable threat to any online presence. The scale and frequency of these attacks have kept increasing over years, partly due to the rise of IoT botnets and the prevalence of cloud infrastructure. The largest documented attack in 2018 has reached 1.35Tbps [2]. Both industry and academic researchers have proposed various solutions to address the DDoS problem. This body of work falls into two main categories: DDoS-resistant network architectures and protection-as-a-service product provided by companies such as Cloudflare and Akamai. Architectural solutions [4] require many upgrades to the existing Internet and have not been widely deployed. A protection-as-a-service product typically uses a large scale global network as a protective “shield” and directs all its customers’ traffic to this network. This shield network is provisioned to have sufficient capacity to withstand the largest anticipated attack. It is expected to filter out attack traffic before the traffic reaches a customer. Despite their effectiveness, those services can be costly. For instance,

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

SIGCOMM Posters and Demos '18, August 20–25, 2018, Budapest, Hungary

© 2018 Association for Computing Machinery.

ACM ISBN 978-1-4503-5915-3/18/08...\$15.00

<https://doi.org/10.1145/3234200.3234232>

Figure 1: The DynaShield architecture

in addition to a flat fee of \$200/month, Cloudflare charges a customer an additional \$0.05 per 10,000 good requests. The service cost can become a financial burden to small or non-profit organizations or individuals.

In this work, we ask the question: can we design a DDoS solution that is free or costs little to an online service provider who cannot readily afford the existing DDoS defense products? Our solution is DynaShield. It exploits the intermittent nature of DDoS attacks and the recent advancements in cloud computing and cryptocurrency to be cost-effective. First, DDoS attacks are often short-lived [1]. Thus we design DynaShield to be an on-demand service. Only when a victim detects an ongoing DDoS attack will DynaShield be triggered so that it introduces no additional cost during peacetime. Second, we use serverless functions (e.g. AWS Lambda) to form a protective shield to protect a victim’s service. During attack times, DynaShield redirects all traffic to this “shield” before it can reach the protected service. Serverless functions can autoscale and are always on, but a customer only pays for the functions get invoked. The autoscaling feature of serverless functions makes them more cost-effective than using a dedicated service such as AWS EC2, since we do not need to use the best available EC2 server to provision for the largest DDoS attack ahead of time. In addition, those cloud services usually provide free raw bandwidth DDoS protection (e.g. AWS Shield). The cloud infrastructure filters out raw bandwidth attack such as UDP flooding and only forward the properly formatted requests to the serverless functions. Finally, the DynaShield design uses cryptocurrency mining as Proof-of-Work (PoW) to help offset the cost of serverless functions. In our design, a cryptocurrency PoW is a puzzle that is difficult to solve but easy to verify. During attack times, each client must produce a share of a cryptocurrency PoW before it can reach the server. This PoW can effectively limit the rate of attack traffic and in the meantime, provide a user a chance to earn mining profit.

2 DYNASHIELD ARCHITECTURE

Figure 1 shows the DynaShield architecture. It has five participating components: clients, DynaShield serverless functions, existing cryptocurrency mining pools, ISP's filtering routers, and the victim servers. Next, we describe DynaShield's operations in more detail.

On-demand DDoS Protection: DynaShield is an on-demand DDoS mitigation solution. During peacetime, clients' traffic would directly reach the protected servers. When a victim detects an ongoing attack or is overload, it will invoke DynaShield, by updating its DNS records to pointing to the serverless functions, and informing its upstream ISPs to install filters (e.g. ACL or BGP Flowspec [5]) that only allow traffic from the serverless functions.

Clients connect to DynaShield: After a victim invokes DynaShield, all subsequent traffic from its clients will first reach the serverless functions.

DynaShield returns puzzles to clients: Before a client can send traffic to the protected server, it must solve a cryptographic puzzle to obtain a capability token. In traditional capability-based DDoS defense solutions [3, 6], the hash-based puzzles generated by the defender have no real value. Differently, DynaShield joins a mining pool as a miner. It divides the cryptocurrency puzzles received from the mining pool into many tiny parts (avoid large overhead on clients) and distributed them to clients as PoW puzzles, which would bring cryptocurrency profit with no cost for DynaShield.

Clients solve puzzles to obtain capabilities: Once a compliant client receives a puzzle, which is in the type of a snippet, it will run it to solve the puzzle and return the result. DynaShield validates its correctness, issues the client a capability token, and records the client together with the status of the token in cloud database (e.g. DynamoDB). A capability token is a cryptographic hash of a client's IP address, the timestamp and TTL value of the token, and the number of requests can be sent with this token. A client's subsequent requests will carry this token. When DynaShield receives a client's request with a capability token, DynaShield will validate it, update the token status, and forward the request.

Blacklisting non-compliant clients: A malicious client may request a puzzle without solving it or send an invalid capability token to DynaShield. In these cases, DynaShield will keep a DB record of clients who repeatedly fail to solve a puzzle or send an invalid capability token as a blacklist, and their traffic will be filtered out at the network layer for a period of time. This mechanism prevents malicious clients from wastefully invoking DynaShield's serverless functions.

3 PRELIMINARY EVALUATION

In our preliminary evaluation, we analyze the cost of DynaShield and compare it with other solutions. We obtain the

statistics of DDoS attacks in 2017 from Imperva Incapsula [1] including attack duration and frequency distribution as well as attack size (requests per second). According to it, we then infer the average number of malicious requests a user receives during a DDoS attack can be estimated as 49 million per month, and the peak as 2853 million per month. We calculate the cost of receiving and processing these numbers of requests using different solutions, namely, DynaShield's serverless functions using the public AWS Lambda pricing information, Cloudflare using the pricing information we obtain from its website, and a dedicated EC2 server. We also estimate the mining profit by assuming that DynaShield receives at least 60 legitimate clients' requests per second. We assume that the legitimate clients always solve the puzzles and malicious requests do not solve any puzzle. In addition, each client has a hashrate of 239H/s, which is half of the hash rate of a commodity PC with an Intel i7-4790 CPU. Menoro Coin is chosen as PoW and its current price at the time of writing is \$191.69. Table 1 shows the result.

per month	peak	average
# of Requests	2853 million	49 million
Cloudflare Cost	-\$14466	-\$477.76
DynaShield Cost	-\$570.65	-\$9.91
EC2 Scheme cost	-\$1758.71	-\$91.63
Menoro Earned	+\$568.8	+\$7.63

Table 1: Cost Comparison

As we can see, DynaShield incurs the list cost on a defender. The profit depends on how long DynaShield works and the number of good clients at any moment. For an average scenario, the mining profit \$7.93 covers most of a defender's cost \$9.91. When a defender is under the largest attack all the time, its monthly cost is \$570.65-\$568.8 $\approx$ \$1.85.

We also evaluate the latency to obtain a cryptocurrency puzzle from the Menoro coin mining pool. If the latency is too large, DynaShield may not obtain a sufficient number of puzzles during a large attack. Fortunately, our experiments show that one can acquire a cryptocurrency puzzle in 9.28 μ s. At this rate, DynaShield can at least 1/9.28 million puzzles per second, even if it does not further divide a cryptocurrency puzzle into smaller parts.

4 CONCLUSION AND FUTURE WORK

In this work, we present DynaShield, an on-demand DDoS defense architecture that uses serverless functions and cryptocurrency PoW to reduce the cost of a defender. Compared to current DDoS mitigation products like Cloudflare, DynaShield has a lower cost.

Our future work will focus on evaluating the latency of updating DNS record and traffic redirection, the cost of monitoring attack during peacetime, and the reaction time of DynaShield when DDoS happens.

REFERENCES

- [1] 2017. Global DDoS Threat Landscape. <https://www.incapsula.com/ddos-report/ddos-report-q1-2017.html>
- [2] 2018. The Hacker News. <https://thehackernews.com/2018/03/biggest-ddos-attack-github.html>
- [3] Colin Dixon, Thomas E Anderson, and Arvind Krishnamurthy. 2008. Phalanx: Withstanding Multimillion-Node Botnets.. In *NSDI*, Vol. 8. 45–58.
- [4] Xin Liu, Xiaowei Yang, and Yong Xia. 2010. NetFence: preventing internet denial of service from inside out. In *ACM SIGCOMM Computer Communication Review*, Vol. 40. ACM, 255–266.
- [5] Pedro Marques, Robert Raszuk, Danny McPherson, Jared Mauch, Barry Greene, and Nischal Sheth. 2009. Dissemination of flow specification rules. *Arbor* (2009).
- [6] Bryan Parno, Dan Wendlandt, Elaine Shi, Adrian Perrig, Bruce Maggs, and Yih-Chun Hu. 2007. Portcullis: protecting connection setup from denial-of-capability attacks. *ACM SIGCOMM Computer Communication Review* 37, 4 (2007), 289–300.