CDN Backfired: Amplification Attacks Based on HTTP Range Requests

2020 50th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)

Authors: Weizhong Li, Kaiwen Shen, Run Guo, Baojun Liu, Jia Zhang, Haixin Duan, Shuang Hao, Xiarun Chen, Yao Wang

Outline

- Introduction
- Background
- Range-specific implementations in CDNs
- Range-based HTTP Amplification attacks
- Real-world evaluation
- Discussion
- Conclusion

Outline

- Introduction
- Background
- Range-specific implementations in CDNs
- Range-based HTTP Amplification attacks
- Real-world evaluation
- Discussion
- Conclusion

Introduction

- CDN v.s. HTTP range request mechanism
  - *The client can not only retrieve partial content of large representations but also efficiently recover from partially failed transfers.*

- two types of Range-based Amplification (RangeAmp) Attacks
  - Small Byte Range (**SBR**) Attack
  - *Overlapping Byte Range (**OBR**) Attack*

Introduction

- Contributions
  - *We present a novel class of HTTP amplification attack, **Range-based Amplification (RangeAmp) Attacks**. The RangeAmp attacks can be used to consume the outgoing bandwidth of victims, which not only downgrades the network availability but also brings economic losses.*
  - *We examine the RangeAmp attacks on 13 popular CDN vendors and evaluate the feasibility and severity of RangeAmp vulnerabilities. We find **all** examined CDNs are vulnerable to the RangeAmp attacks, and the amplification factor is up to 43000 times in some cases.*
  - *We also responsibly disclosed all security issues to affected CDN vendors. Further, we analyze the root cause of RangeAmp vulnerabilities and **propose countermeasures and mitigation solutions**.*

Outline

- Introduction
- Background
- Range-specific implementations in CDNs
- Range-based HTTP Amplification attacks
- Real-world evaluation
- Discussion
- Conclusion

Background

- CDN Overview

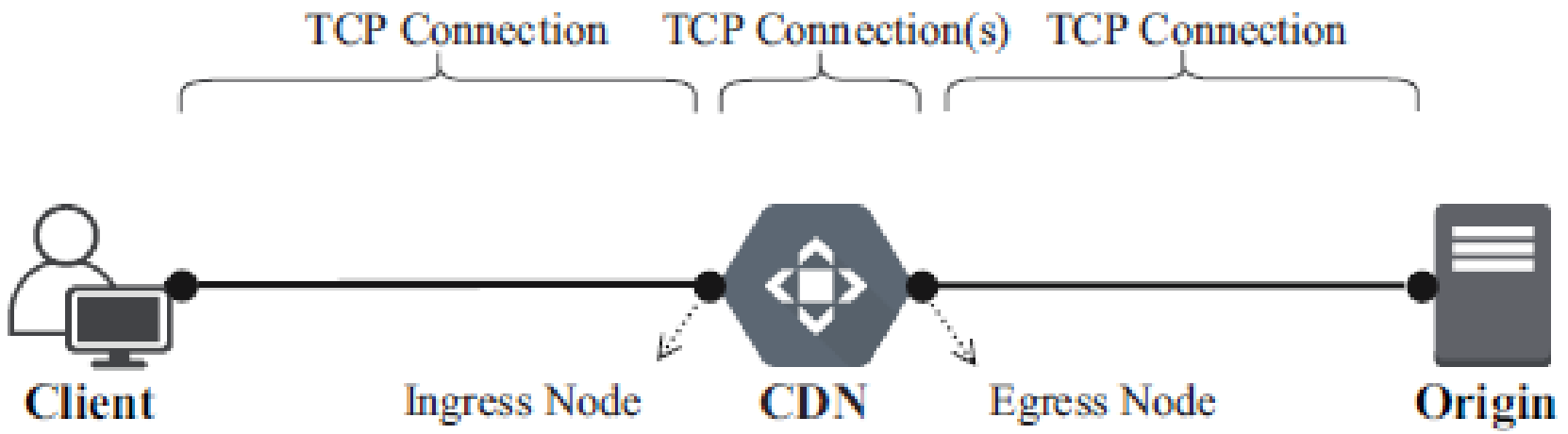


Fig. 1. Multiple segments of connectivity in a CDN environment

Background

- HTTP Range Request Mechanism
  - *Because of canceled requests or dropped TCP connections, HTTP clients often encounter interrupted data transfers.*
  - *Range requests allow clients to efficiently recover from partially failed transfers and retrieve partial content of large resources, effectively reducing unnecessary data transmission.*

Background

- HTTP Range Request Mechanism

```
1 GET /1KB.jpg HTTP/1.1
2 Host: example.com
3 Range: bytes=0-0
4
5
```

(a) range request with a single byte range

```
1 GET /1KB.jpg HTTP/1.1
2 Host: example.com
3 Range: bytes=1-1,-2
4
5
```

(b) range request with multiple byte ranges

```
1 HTTP/1.1 206 OK
2 Content-Length: 1
3 Accept-Ranges: bytes
4 Content-Type: image/jpeg
5 Content-Range: bytes 0-0/1000
6
7 \xff
```

(c) 206 response to the request in (a)

```
1  HTTP/1.1 206 OK
2  Content-Length: 208
3  Accept-Ranges: bytes
4  Content-Type: multipart/byteranges;
   boundary=THIS_STRING_SEPARATES
5
6
7  --THIS_STRING_SEPARATES
8  Content-Type: image/jpeg
9  Content-Range: bytes 1-1/1000
10
11 \xff
12 --THIS_STRING_SEPARATES
13 Content-Type: image/jpeg
14 Content-Range: bytes 998-999/1000
15
16 f\x00
17 --THIS_STRING_SEPARATES--
18
```

(d) multipart response to the request in (b)

Fig. 2. Examples of range requests and partial responses

Outline

- Introduction
- Background
- Range-specific implementations in CDNs
- Range-based HTTP Amplification attacks
- Real-world evaluation
- Discussion
- Conclusion

Range-specific implementations in CDNs

- Differences in CDNs Handling Range Requests
  - ***Laziness*** – *Forward the Range header without change.*
  - ***Deletion*** – *Remove the Range header directly.*
  - ***Expansion*** – *Extend it to a larger scale of byte range.*

- When receiving a range request, most CDNs prefer to adopt the **Deletion** policy or the **Expansion** policy because they believe that the client may continue requesting other byte ranges of the same resource.

Range-specific implementations in CDNs

- RFC2616
  - *Places no restrictions on multi-range requests.*
  - *The "Apache Killer", known as CVE-2011-3192, can exhaust memory on the Apache server by creating a number of threads that use a Range header with multiple ranges.*
- RFC7233
  - *Adds some security considerations to multi-range requests.*
    - An HTTP server ought to ignore, coalesce, or reject range requests with **more than two overlapping ranges or many small ranges** in the Range header.
  - *However, some CDNs ignore it.*

Outline

- Introduction
- Background
- Range-specific implementations in CDNs
- Range-based HTTP Amplification attacks
- Real-world evaluation
- Discussion
- Conclusion

Range-based HTTP Amplification attacks

- Threat Model

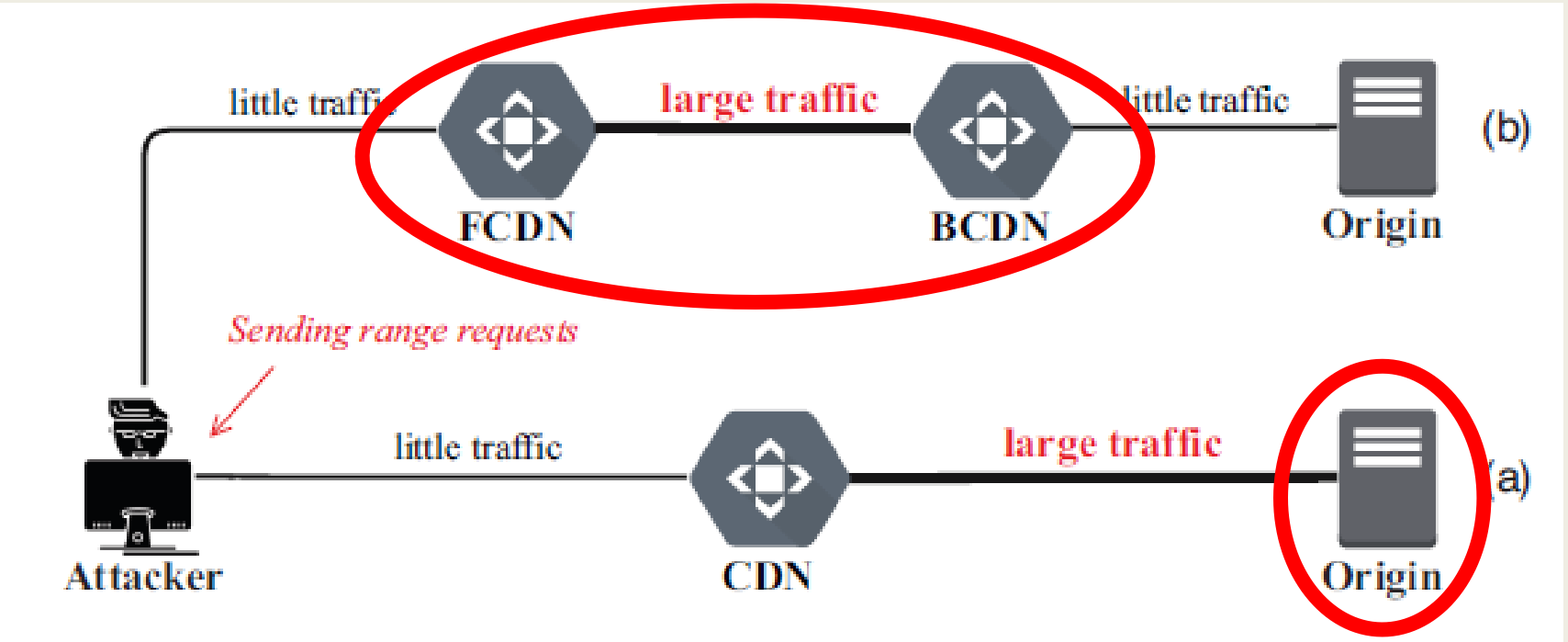


Fig. 3. *General construction of the RangeAmp Attacks*

Range-based HTTP Amplification attacks

- Case (a): Small Byte Range(SBR) Attack
  - *If a CDN adopts the Deletion or Expansion policy to handle range requests, an attacker can craft a Range header with a small byte range to launch SBR attack.*
  - ***The bigger the target resource, the larger the amplification factor**.*

Range-based HTTP Amplification attacks

- Case (a): Small Byte Range(SBR) Attack

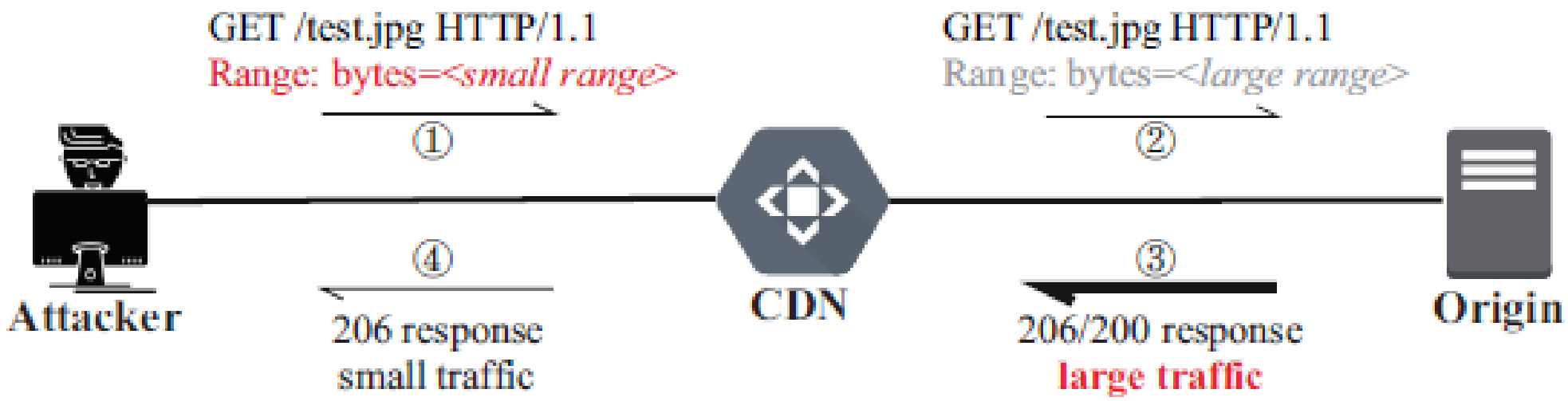


Fig. 4. *Flow and example construction of the SBR Attack*

Range-based HTTP Amplification attacks

- Case (b): Overlapping Byte Ranges(OBR) Attack
  - *If the FCDN adopts the Laziness policy and the BCDN returns a multi-part response without checking whether ranges overlap, an attacker can craft a Range header with multiple overlapping byte ranges to launch OBR attack.*
  - ***The greater the number of overlapping ranges, the larger the amplification factor.***

Range-based HTTP Amplification attacks

- Case (b): Overlapping Byte Ranges(OBR) Attack

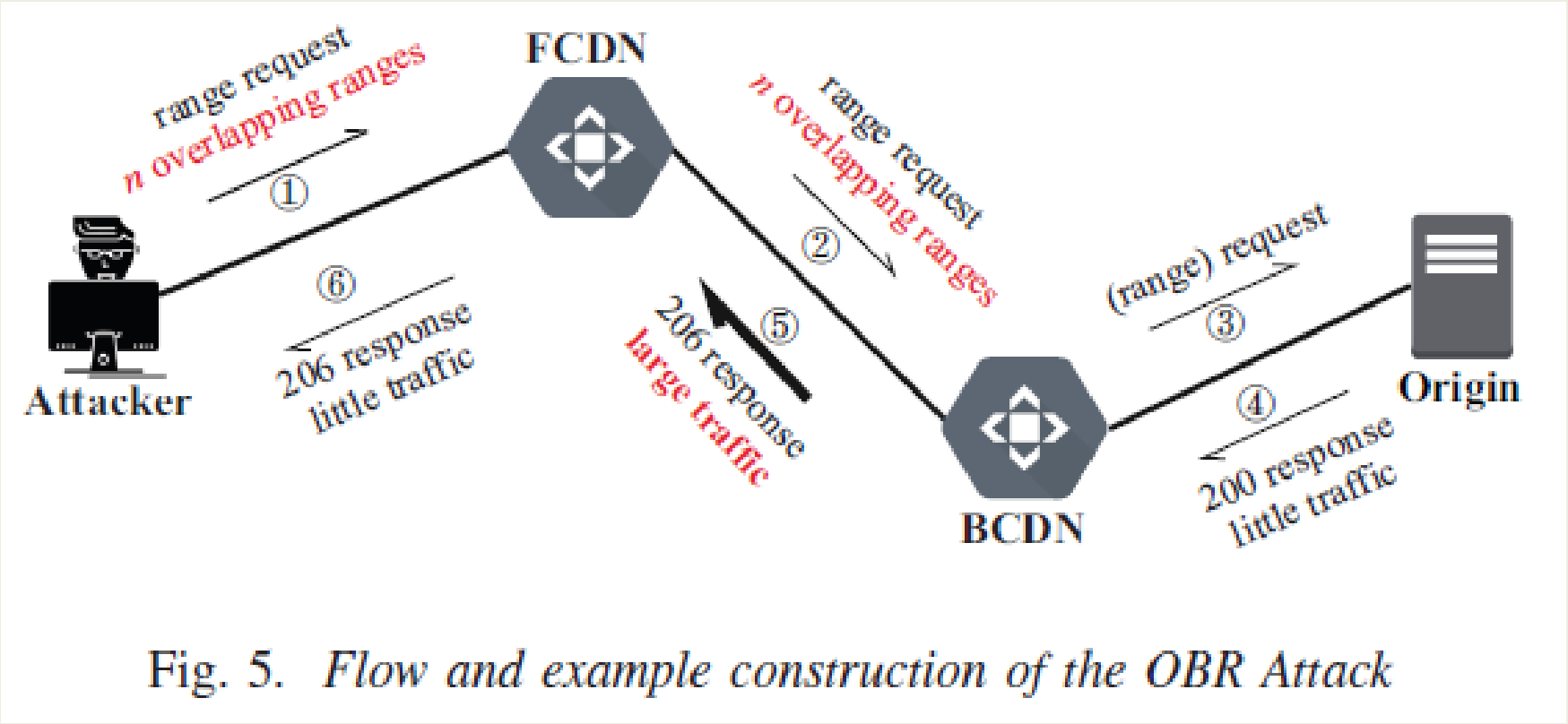


Fig. 5. *Flow and example construction of the OBR Attack*

Outline

- Introduction
- Background
- Range-specific implementations in CDNs
- Range-based HTTP Amplification attacks
- Real-world evaluation
- Discussion
- Conclusion

Real-world evaluation

- Feasibility of the RangeAmp Attacks
- The Amplification Factor of the SBR Attack
- The Amplification Factor of the OBR Attack
- Practicability of the RangeAmp Attacks
- Severity Assessment

Feasibility of the RangeAmp Attacks

- Test the actual range-specific policies of each CDN to figure out which CDNs are vulnerable to the SBR and/or OBR attack.

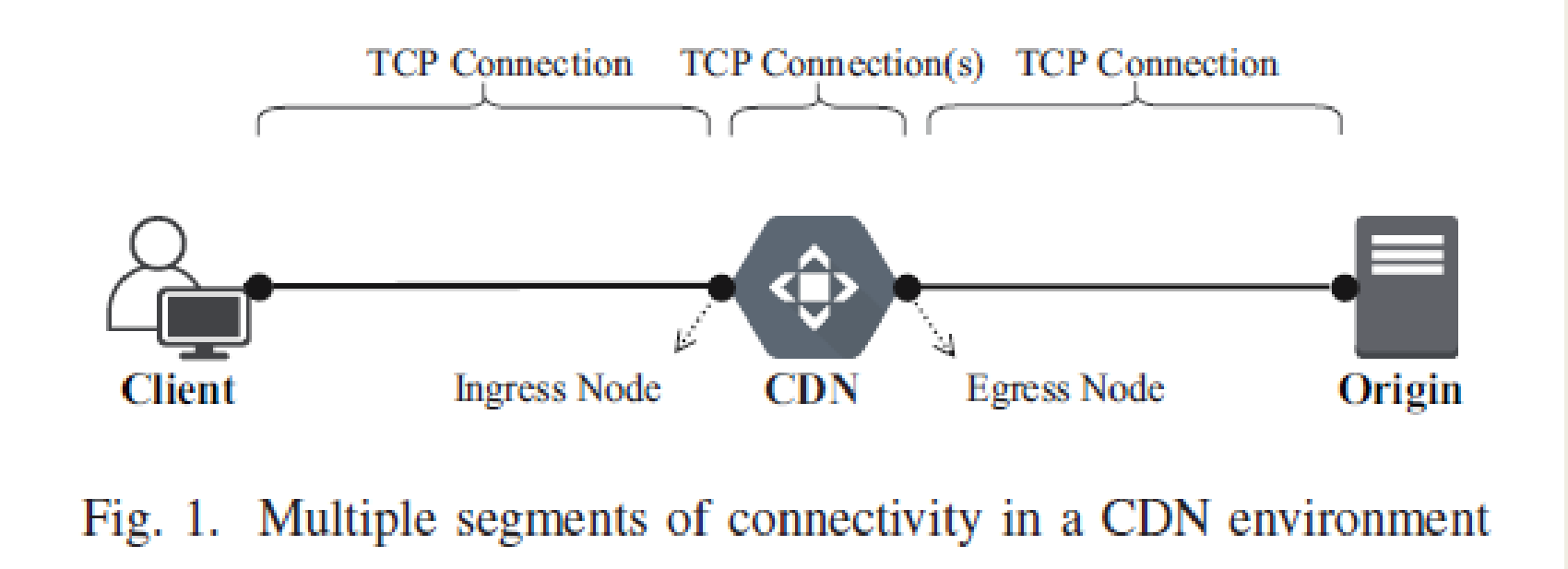


Fig. 1. Multiple segments of connectivity in a CDN environment

Feasibili acks

TABLE I
RANGE FORWARDING BEHAVIORS VULNERABLE TO SBR ATTACK

CDN	Vulnerable Range Format	Forwarded Range Format
Akamai	bytes=first-last bytes=-suffix	None None
Alibaba Cloud	bytes=-suffix	None (*)
Azure	bytes=first-last (F$\leq$8MB) bytes=8388608-8388608 (F$>$8MB)	None None & bytes=8388608-16777215
CDN77	bytes=first-last (first$<$1024)	None
CDNsun	bytes=0-last	None
Cloudflare	bytes=first-last bytes=-suffix	None (*) None (*)
CloudFront	bytes=first-last bytes=$first_1$-$last_1$,...,$first_n$-$last_n$	bytes=$first'$-$last'$ bytes=$first'$-$last'$
Fastly	bytes=first-last bytes=-suffix	None None
G-Core Labs	bytes=first-last bytes=-suffix	None None
Huawei Cloud	bytes=-suffix (F$<$10MB) bytes=first-last (F$\geq$10MB)	None (*) None & None (*)
KeyCDN	bytes=first-last (& bytes=first-last)	bytes=first-last (& None)
StackPath	bytes=first-last bytes=-suffix	bytes=first-last [& None] bytes=first-last [& None]
Tencent Cloud	bytes=first-last	None (*)

Note: F is the file size of the target resource.

Feasibility of the RangeAmp Attacks

TABLE II
RANGE FORWARDING BEHAVIORS VULNERABLE TO OBR ATTACK

CDN	Vulnerable Range Format	Forwarded Range Format
CDN77	bytes=start$_1$-,start$_2$-,...,start$_n$- (start$_1 \geq$1024)	Unchanged
CDNsun	bytes=start$_1$-,start$_2$-,...,start$_n$- (start$_1 \geq$1)	Unchanged
Cloudflare	bytes=start$_1$-,start$_2$-,...,start$_n$-	Unchanged (*)
StackPath	bytes=start$_1$-,start$_2$-,...,start$_n$-	Unchanged [& None]

TABLE III
RANGE REPLYING BEHAVIORS VULNERABLE TO OBR ATTACK

CDN	Vulnerable Ranges Format	Response Format
Akamai	bytes=start$_1$-,start$_2$-,...,start$_n$-	n-part response (overlapping)
Azure	bytes=start$_1$-,start$_2$-,...,start$_n$- ($n \leq$64)	n-part response (overlapping)
StackPath	bytes=start$_1$-,start$_2$-,...,start$_n$-	n-part response (overlapping)

Real-world evaluation

- Feasibility of the RangeAmp Attacks
- The Amplification Factor of the SBR Attack
- The Amplification Factor of the OBR Attack
- Practicability of the RangeAmp Attacks
- Severity Assessment

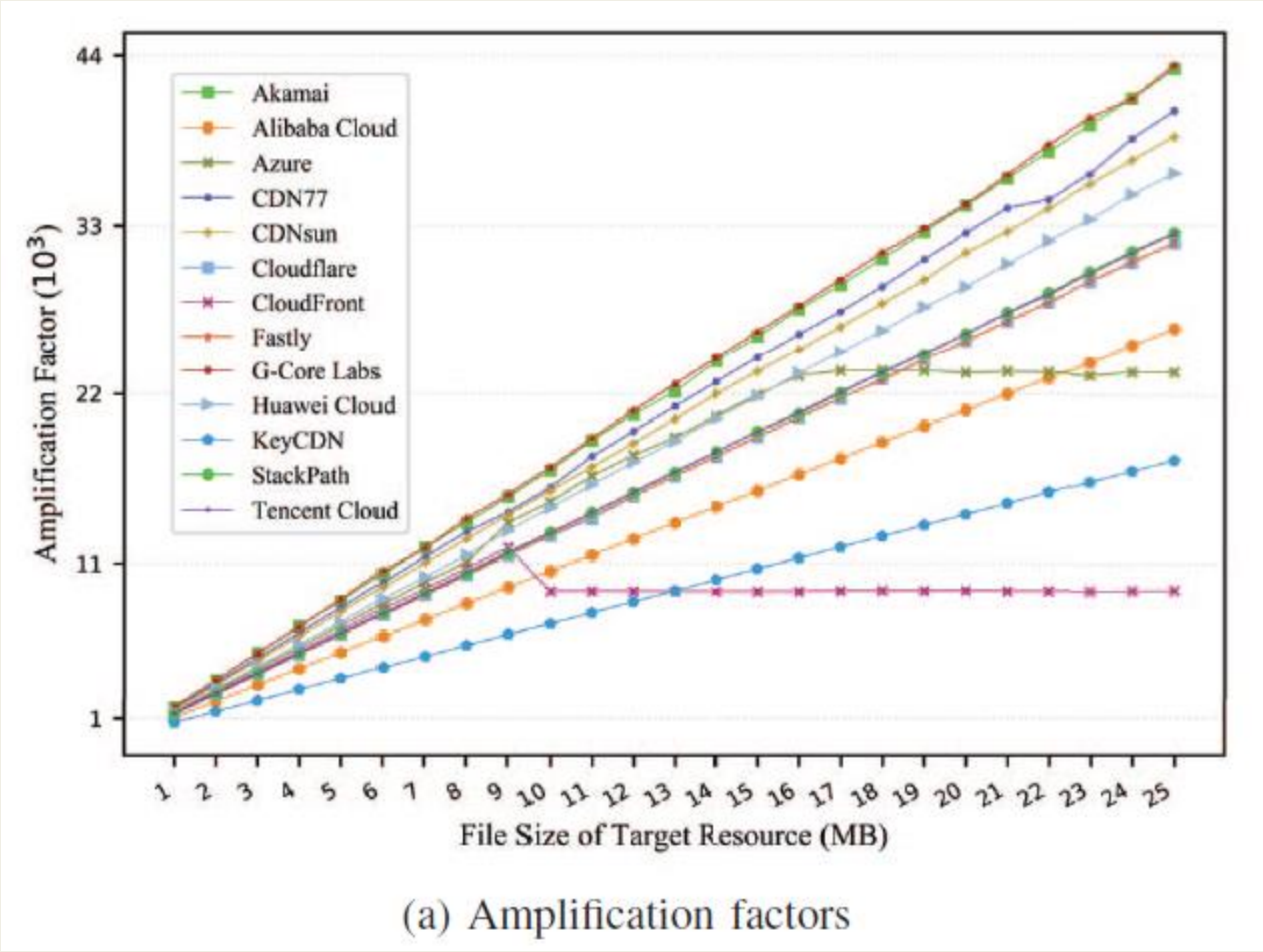
The Amplification Factor of the SBR Attack

TABLE IV
THE AMPLIFICATION FACTOR VARIES WITH THE FILE SIZE OF THE TARGET RESOURCE IN THE SBR ATTACK.

CDN	Exploited Range Case	Amplification Factor		
		1MB	*10MB*	*25MB*
Akamai	bytes=0-0	1707	16991	43093
Alibaba Cloud	bytes=-1	1056	10498	26241
Azure	bytes=0-0 (F≤8MB) bytes=8388608-8388608 (F>8MB)	1401	15016	23481
CDN77	bytes=0-0	1612	15915	40390
CDNsun	bytes=0-0	1578	15705	38730
Cloudflare	bytes=0-0	1282	12791	31836
CloudFront	bytes=0-0,9437184-9437184	1356	9214	9281
Fastly	bytes=0-0	1286	12836	31820
G-Core Labs	bytes=0-0	1763	17197	43330
Huawei Cloud	bytes=-1 (F<10MB) bytes=0-0 (F≥10MB)	1465	14631	36335
KeyCDN	bytes=0-0 & bytes=0-0	724	7117	17744
StackPath	bytes=0-0	1297	13007	32491
Tencent Cloud	bytes=0-0	1308	12997	32438

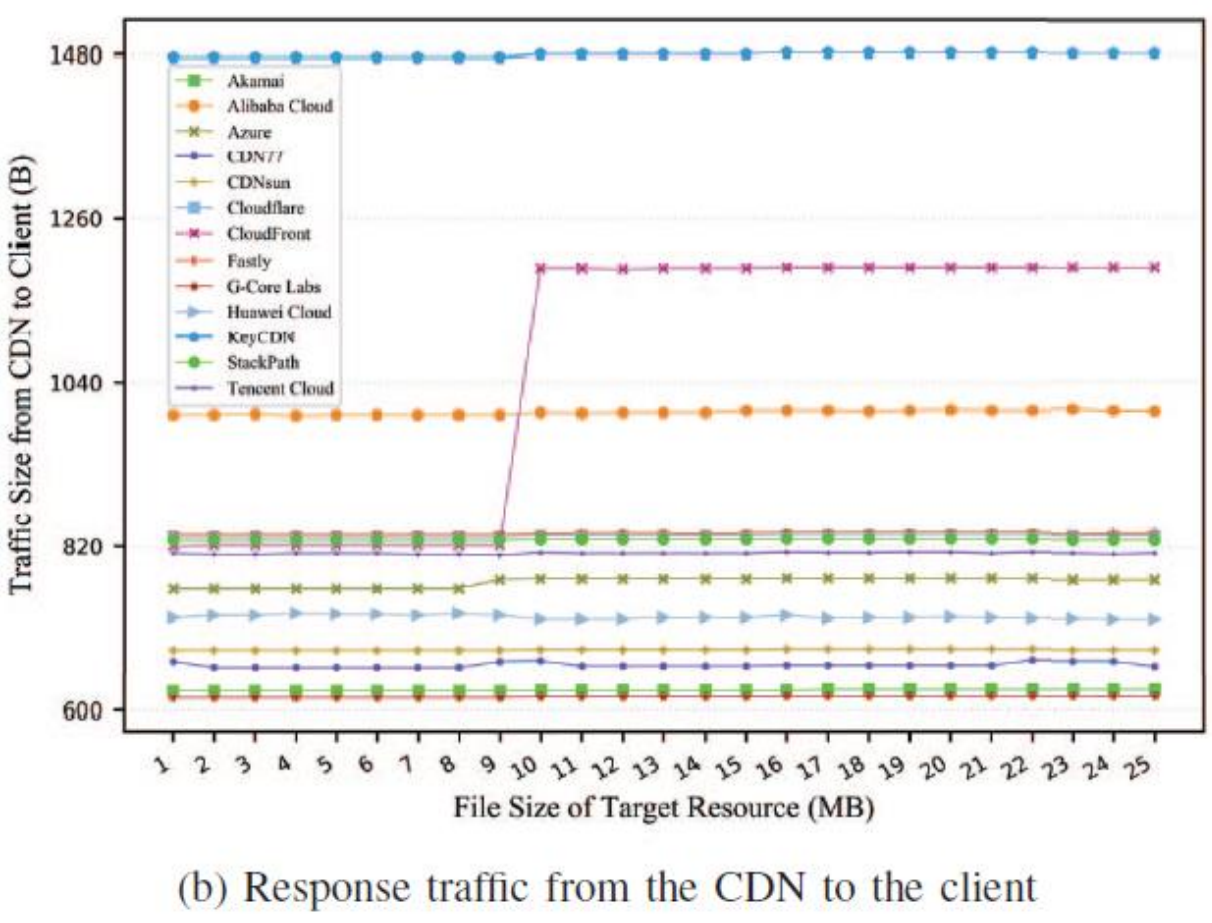
Note: F is the file size of the target resource.

The Amplification Factor of the SBR Attack

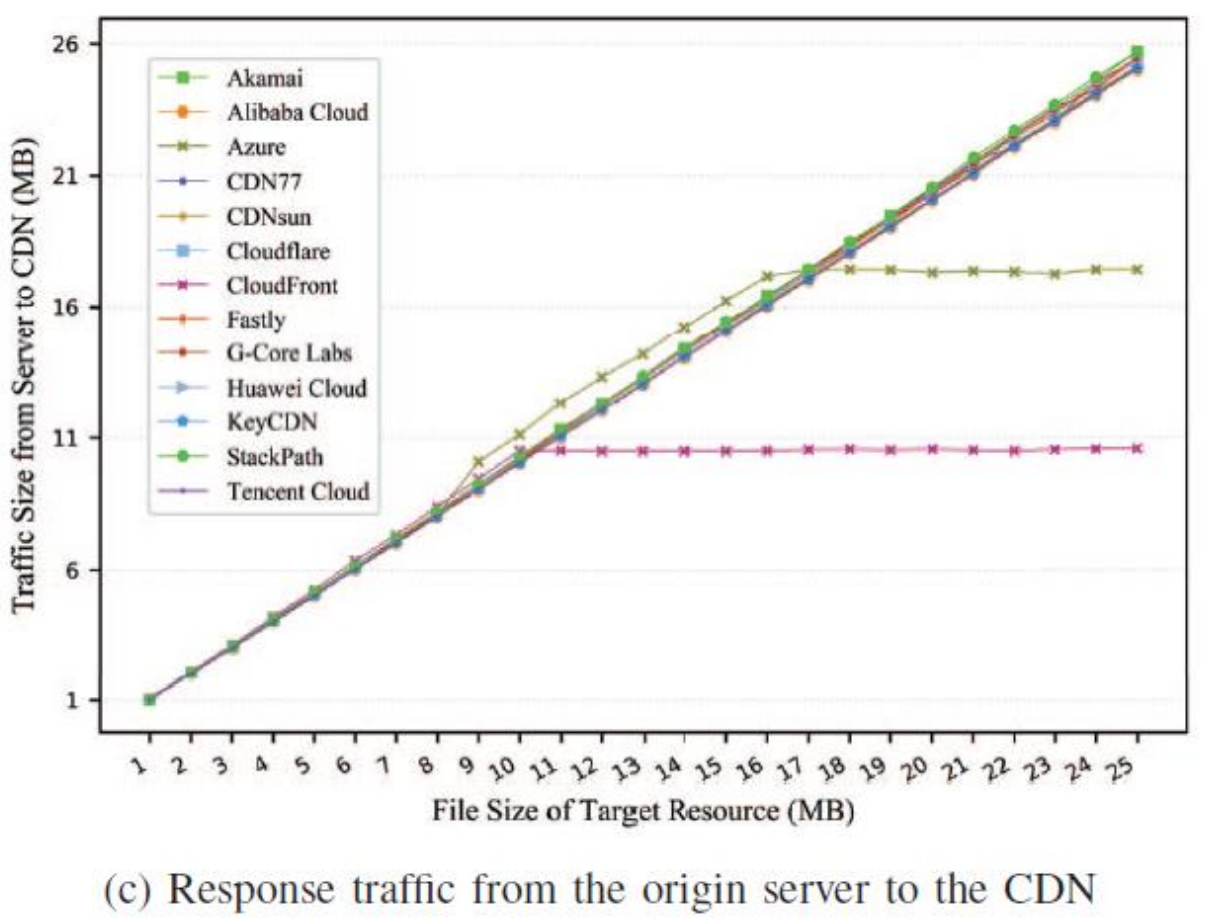


(a) Amplification factors

The Amplification Factor of the SBR Attack



(b) Response traffic from the CDN to the client



(c) Response traffic from the origin server to the CDN

Real-world evaluation

- Feasibility of the RangeAmp Attacks
- The Amplification Factor of the SBR Attack
- The Amplification Factor of the OBR Attack
- Practicability of the RangeAmp Attacks
- Severity Assessment

The Amplification Factor of the OBR Attack

TABLE V
THE MAX AMPLIFICATION FACTOR OF THE OBR ATTACK

FCDN	BCDN	Exploited Range Case	Max n	Exploiting with 1KB of Target Resource and Max n		
				Traffic from Server to BCDN	*Traffic from BCDN to FCDN*	*Amplification Factor*
CDN77	Akamai	bytes=-1024,0-,...,0-	5455	1676B	6350944B	3789.35
	Azure		64	1620B	86745B	53.55
	StackPath		5455	1808B	6413097B	3547.07
CDNsun	Akamai	bytes=1-,0-,...,0-	5456	1676B	6337810B	3781.51
	Azure		64	1620B	84481B	52.15
	StackPath		5456	1808B	6414011B	3547.57
Cloudflare	Akamai	bytes=0-,0-,...,0-	10750	1676B	12456915B	7432.53
	Azure		64	1620B	85386B	52.71
	StackPath		10750	1940B	12636554B	6513.69
StackPath	Akamai	bytes=0-,0-,...,0-	10801	1676B	12522091B	7471.41
	Azure		64	1620B	82191B	50.74
	StackPath		-	-	-	-

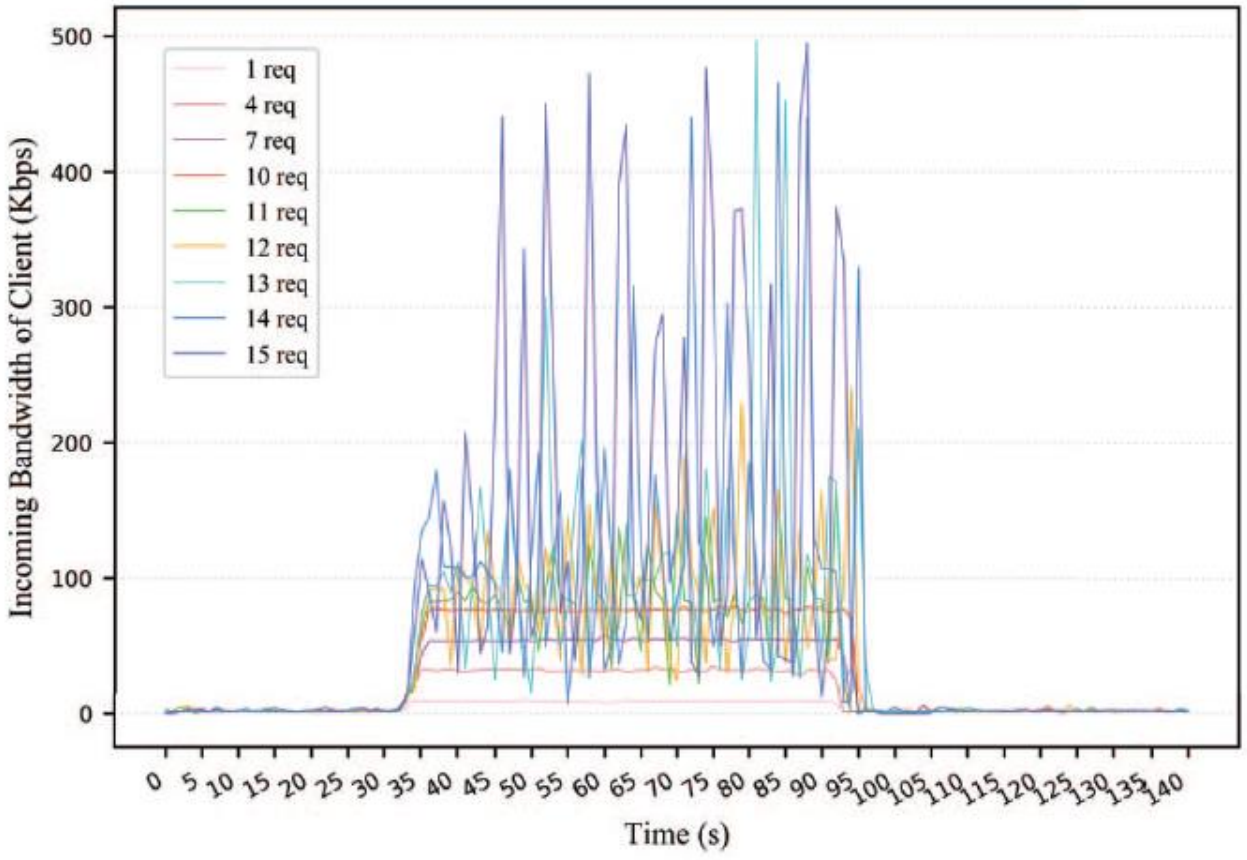
Note: n is the number of overlapping ranges in the exploited multi-range request.

Real-world evaluation

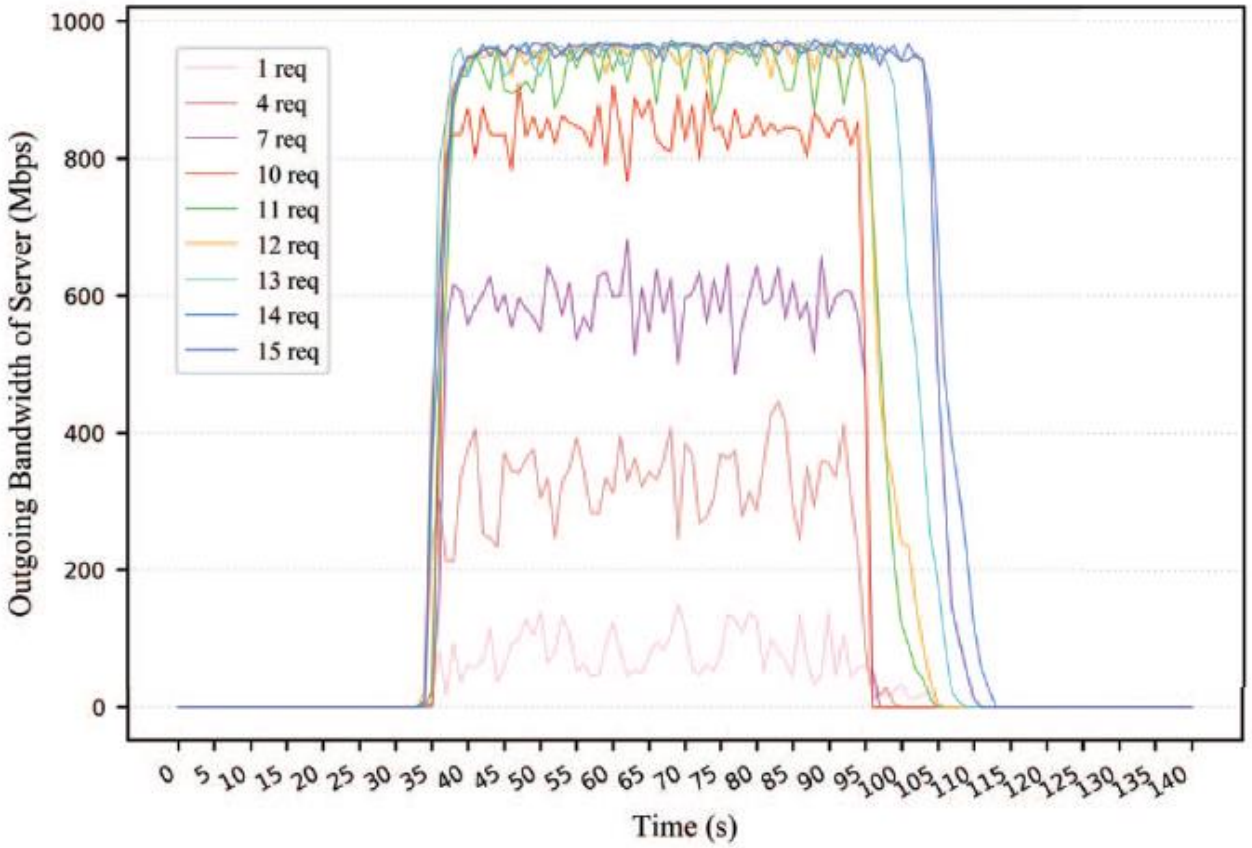
- Feasibility of the RangeAmp Attacks
- The Amplification Factor of the SBR Attack
- The Amplification Factor of the OBR Attack
- Practicability of the RangeAmp Attacks
- Severity Assessment

Practicability of the RangeAmp Attacks

- Evaluate the SBR attack's damage to bandwidth



(a) Incoming bandwidth consumption of the client



(b) Outgoing bandwidth consumption of the origin server

Real-world evaluation

- Feasibility of the RangeAmp Attacks
- The Amplification Factor of the SBR Attack
- The Amplification Factor of the OBR Attack
- Practicability of the RangeAmp Attacks
- Severity Assessment

Severity Assessment

- All 13 CDNs we tested are vulnerable to the SBR attack, and 11 combinations of cascaded CDNs are vulnerable to the OBR attack
- Low-cost and efficient DDoS attack
- Great monetary loss to the victims.
- Traditional DDoS attacks that consume bandwidth mainly target the victim's incoming bandwidth. Instead, The RangeAmp attacks mainly consume the victim's **outgoing** bandwidth.

Outline

- Introduction
- Background
- Range-specific implementations in CDNs
- Range-based HTTP Amplification attacks
- Real-world evaluation
- Discussion
- Conclusion

Discussion

- Ethic Consideration
  - *In the 1st and 2nd experiments, only send one range request to the CDN each time, which hardly affects the CDN's performance.*
  - *In the 3rd experiment, the target resource size is just 1KB, which will not generate excessive traffic in the fcdn-bcdn connection after being enlarged.*
  - *In the 4th experiment, send all requests to completely different ingress nodes of the CDN to minimize or avoid real impacts on the performance of specific nodes. And sustain the experiment for only 30 seconds each time to keep the bandwidth consumption as little as possible.*

Discussion

- Root Cause Analysis
  - *RFC7233 realizes that the range-introduced efficiency could also bring DoS attacks against the server and gives some suggestions on multi-range requests. However, it does not clearly define how CDNs should handle a Range header.* Leading to the **SBR attack**.
  - *RFC7233 has already warned about the threat caused by overlapping byte ranges but some CDNs ignore it, causing the **OBR attack**.*

Discussion

- Mitigation
  - ***Server side: Enforce local DoS defense***
    - Does not necessarily work. From the perspective of the origin server, attack requests are no different from benign requests and come from widely distributed CDN nodes. It is difficult for the origin server to defend against it effectively without affecting normal services.
  - ***CDN side: Modify the specific implementation on range requests***
    - SBR: The essential approach is to improve the policy of handling the Range header.
      - *Adopt the Expansion policy but not extend the byte range too much.*
    - OBR: Follow the security recommendations on multirange requests in RFC7233
  - ***Protocol side: Revise a well-defined and security-aware RFC***
    - A more specific limit of the Range header should be defined in a future updated RFC.

Outline

- Introduction
- Background
- Range-specific implementations in CDNs
- Range-based HTTP Amplification attacks
- Real-world evaluation
- Discussion
- Conclusion

Conclusion

- We find that the 13 popular CDNs tested are all vulnerable. The unclear definition and security negligence of the specifications are the root cause, and the implementation flaws of CDNs further worsen this vulnerability.
- The RangeAmp attacks can pose severe threats to the serviceability of CDNs and the availability of websites.
- A more specific limit of range requests should be defined in a future updated RFC, especially for the HTTP middle-boxes like CDNs.