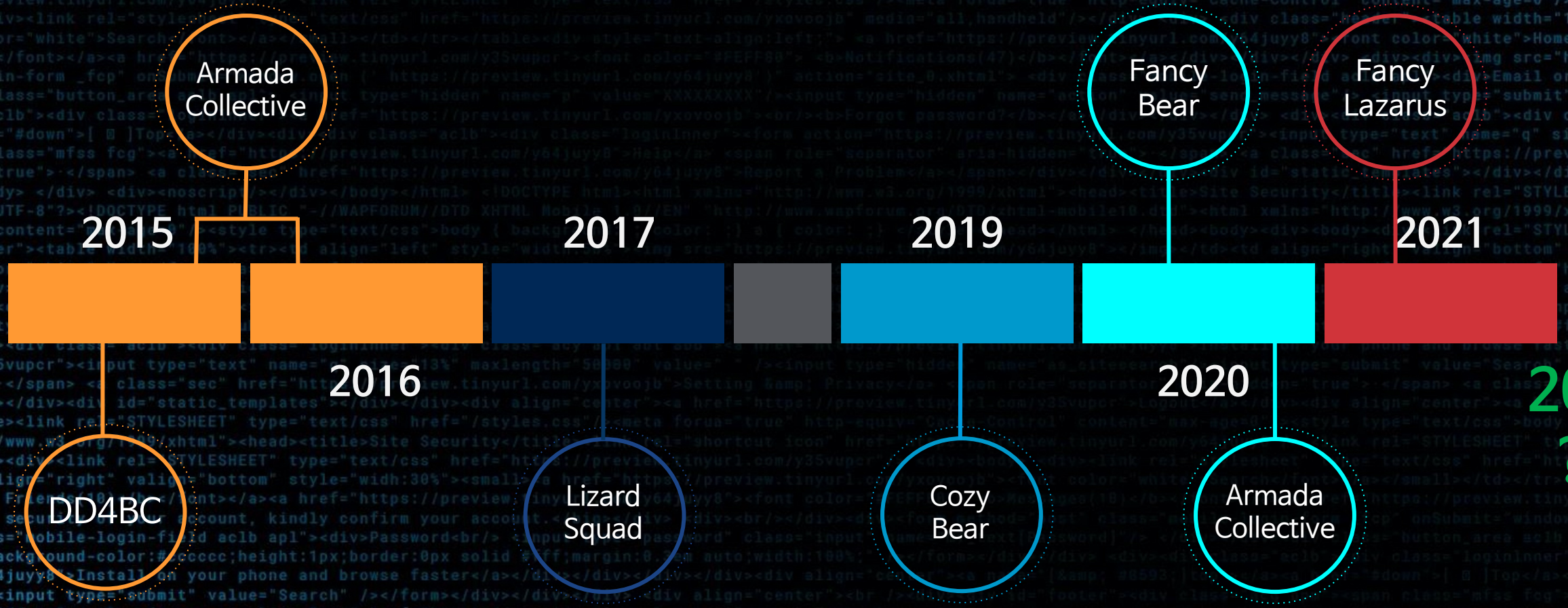
TCP 미들박스 반사 증폭 공격

https://brunch.co.kr/magazine/itsecurity



Source: www.akamai.com

TCP 미들박스 반사 증폭 공격

TCP 미들박스(middlebox) 반사 증폭 DDoS 공격

- 2021년 8월 연구 발표, 2022년 3월 발견
- 반사(reflected) + 증폭(amplification) =〉 DDoS
- 인터넷상에 분포된 미들박스의 TCP 구현 오류를 이용한 공격
- TCP handshake 종료 이전에 HTTP 응답을 제공하는 오류
- 공격자는 최소의 노력으로 최대의 증폭을 만들어낼 수 있음(51,000배)
- Akamai 관측 초당 1.5Mpps, 11Gbps까지 발견
- 실제로는 무한 루프 증폭도 가능

TCP 미들박스

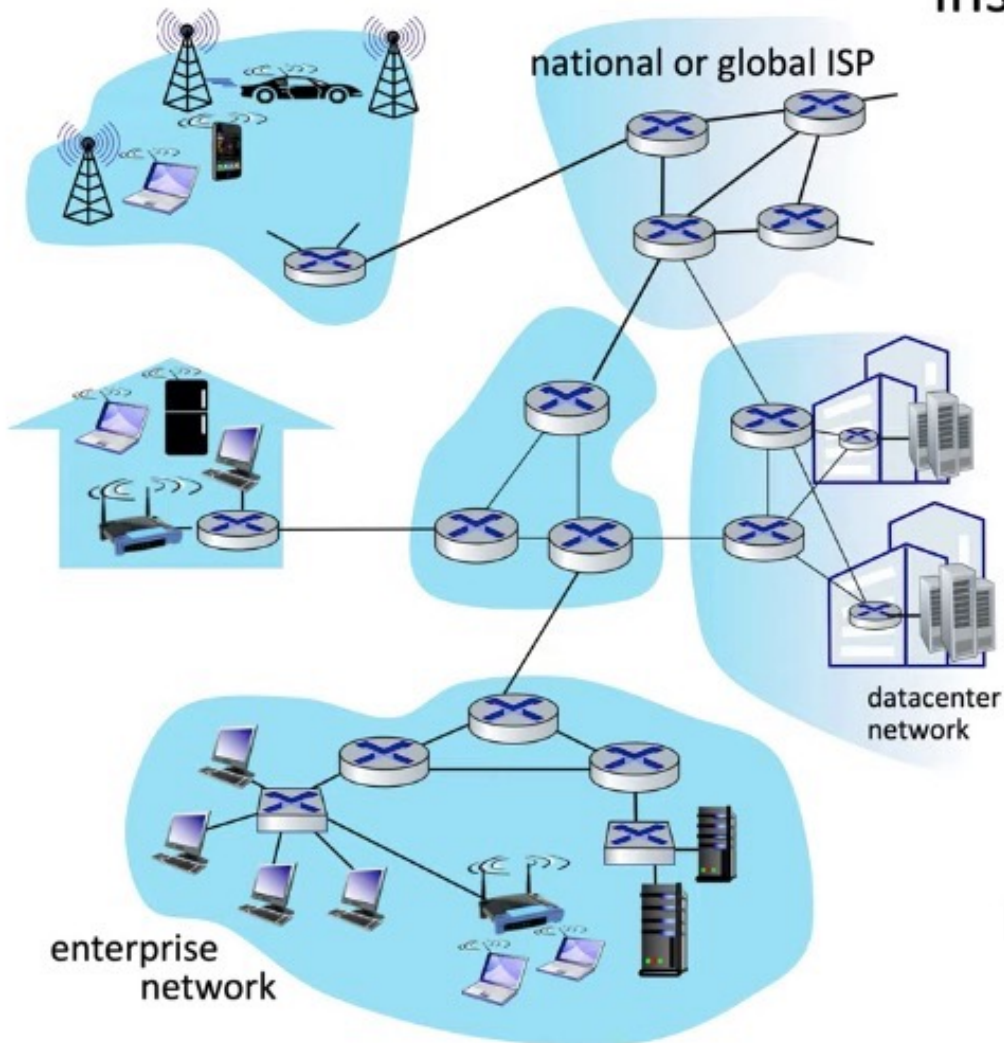
RFC 3234

"middleboxes" – defined as any intermediary box
Performing functions apart from normal, standard functions of
An IP router on the data path between
A source host and destination host.

Middleboxes everywhere!

NAT: home, cellular, institutional

Application-specific: service providers, institutional, CDN



Firewalls, IDS: corporate, institutional, service providers, ISPs

Load balancers: corporate, service provider, data center, mobile nets

Caches: service provider, mobile, CDNs

TCP 미들박스

- 통신하는 두 endpoint의 경로 중간에서 전송 중인 패킷 스트림을 모니터링, 필터링 또는 변환하는 장치
- 패킷의 헤더 뿐만 아니라 Payload도 확인할 수 있음 예) DPI
- 방화벽, IDS, 웹 검열 시스템 등에 사용
- 주로 ISP별로 운영 하거나 국가별 네트워크 가장 자리(국가 검열)에 위치

TCP 미들박스

일반적으로 보안 혹은 성능의 목적으로 사용되는 네트워크 장치

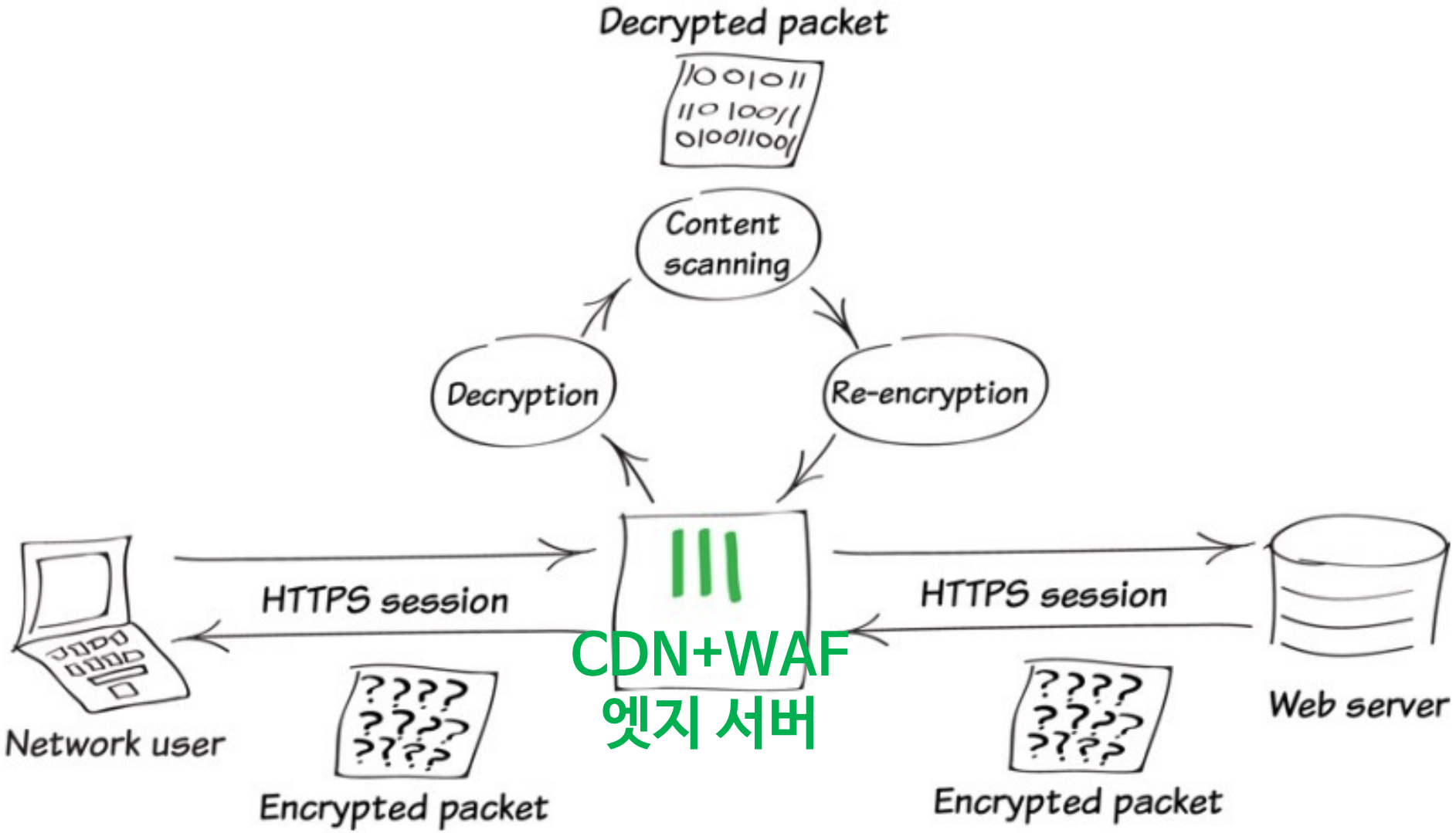
- 네트워크 방화벽
- 웹 방화벽
- 침입 탐지 시스템(IDS)
- 침입 차단 시스템(IPS)

- 프록시(Proxy) 서버
- 캐싱 서버
- CDN(Content Delivery Network)
- WAN 최적화 솔루션
- 프로토콜 가속기

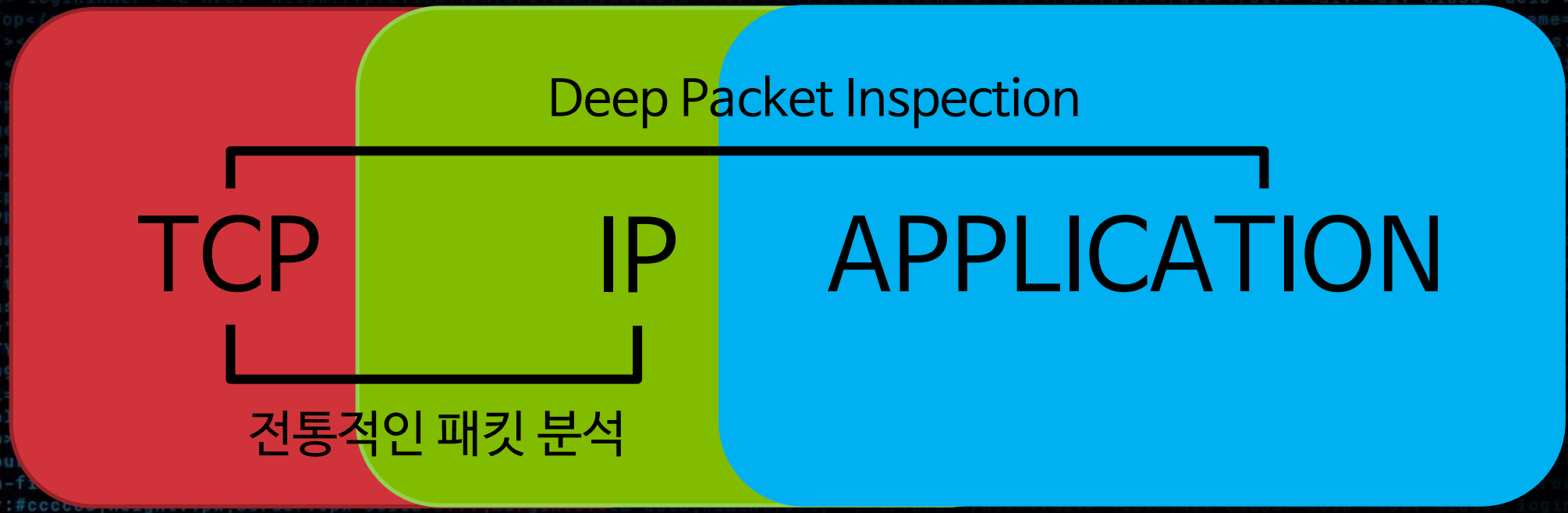
기타

- 네트워크 모니터링
- 인터넷 콘텐츠 검열
- NAT(Network Address Translator)

TCP 미들박스 예제 - CDN/WAF



TCP 미들박스 예제 - DPI(Deep Packet Inspection)

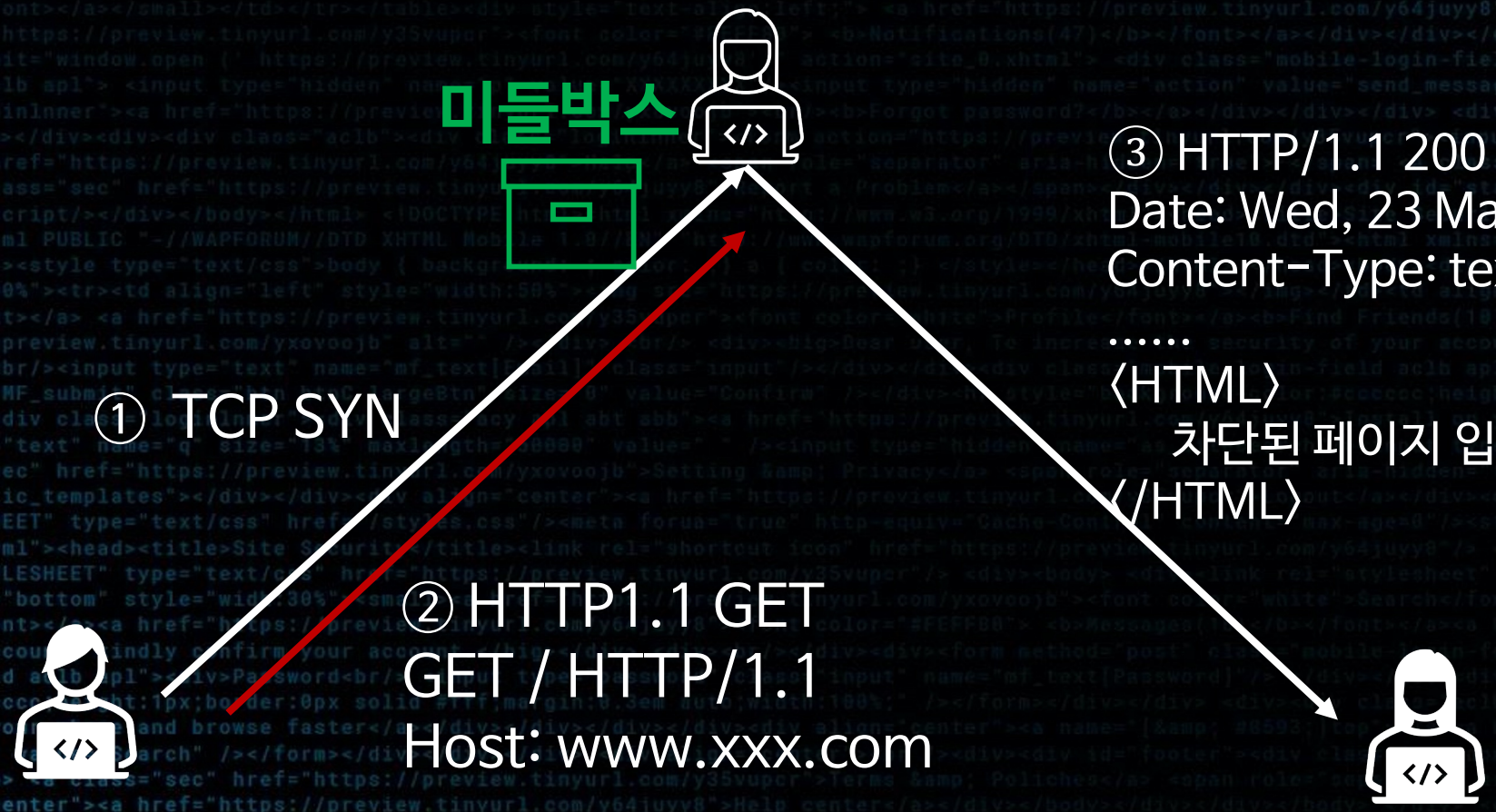


Layer 3 + Layer 4 + Layer 7

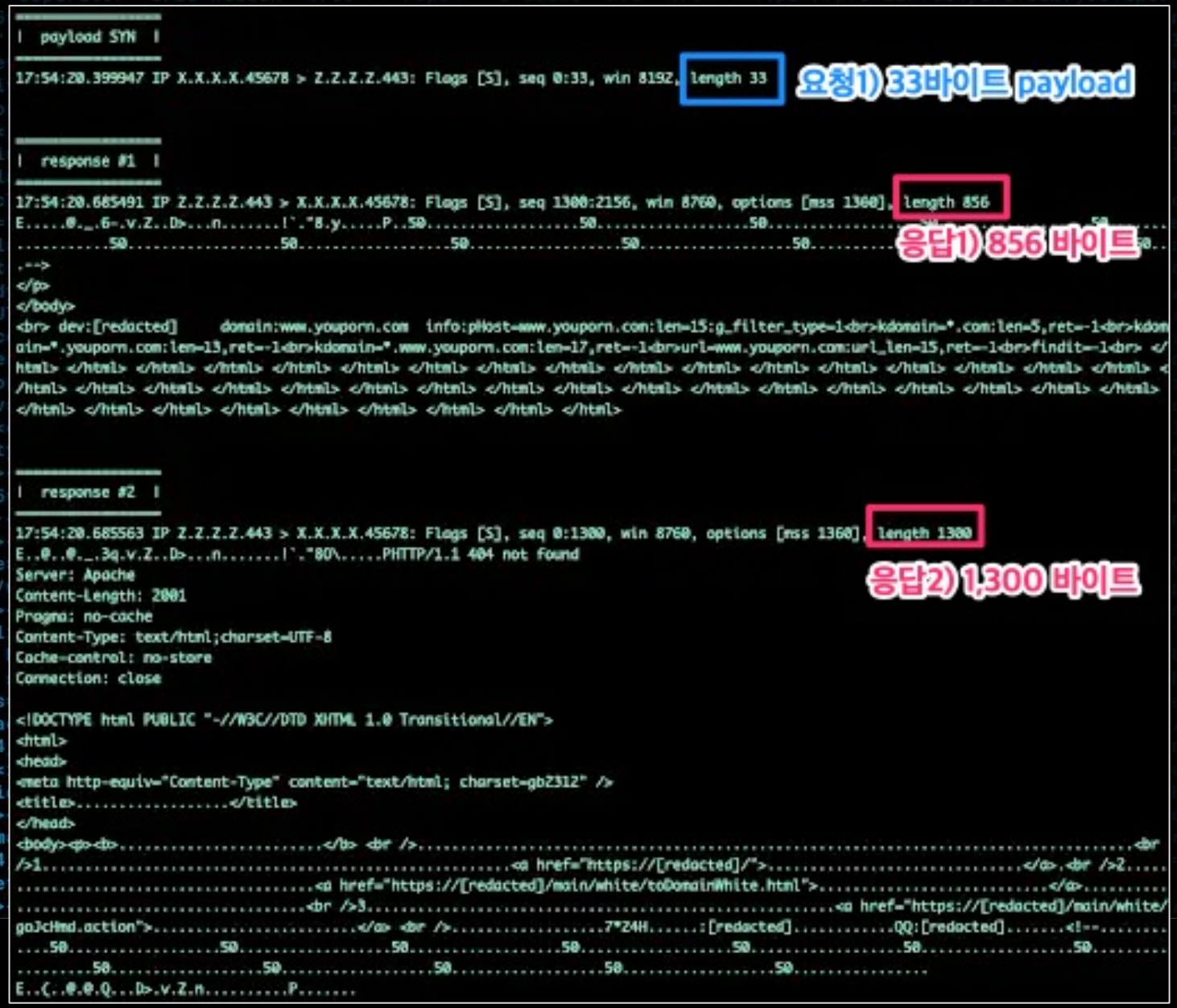
공격에 사용된 TCP 미들박스의 취약점

- 상당수의 미들박스가 TCP 표준을 지키고있지 않음
- TCP 3Way HandShake를 수행하지 않음
- TCP 연결이 완료되지 않은 상태에서 HTTP 요청을 받음
- 결과적으로 유효한 TCP 연결없이 HTTP GET 요청에 응답 수행

TCP 미들박스 반사 증폭 공격



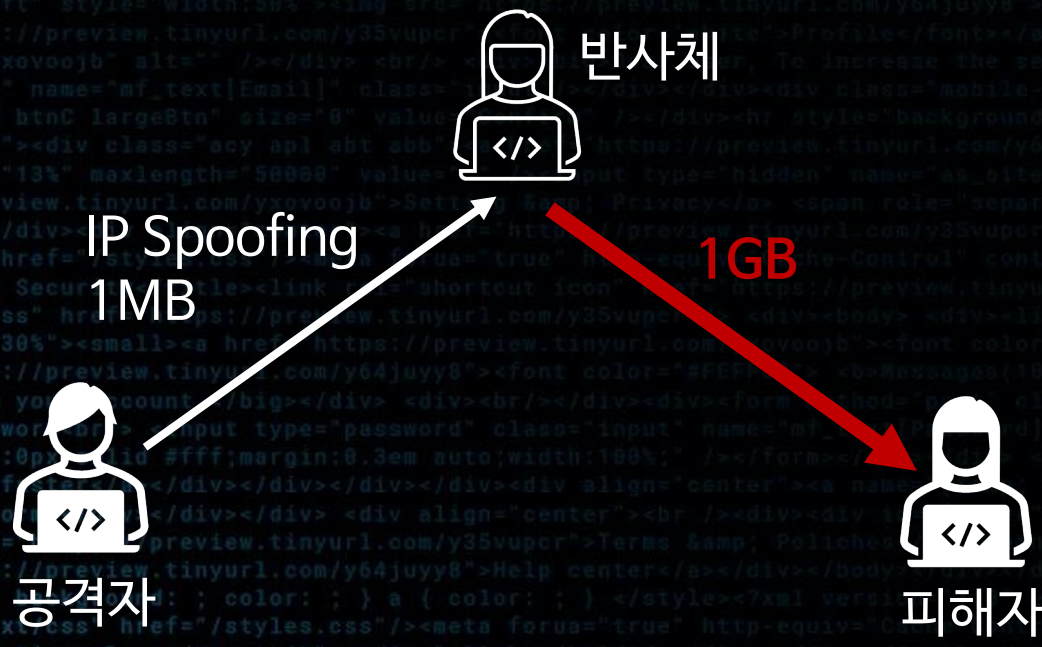
TCP 미들박스 반사 증폭 공격



예제의 증폭 계수:
(856 + 1,300) / 33 = 65.3배

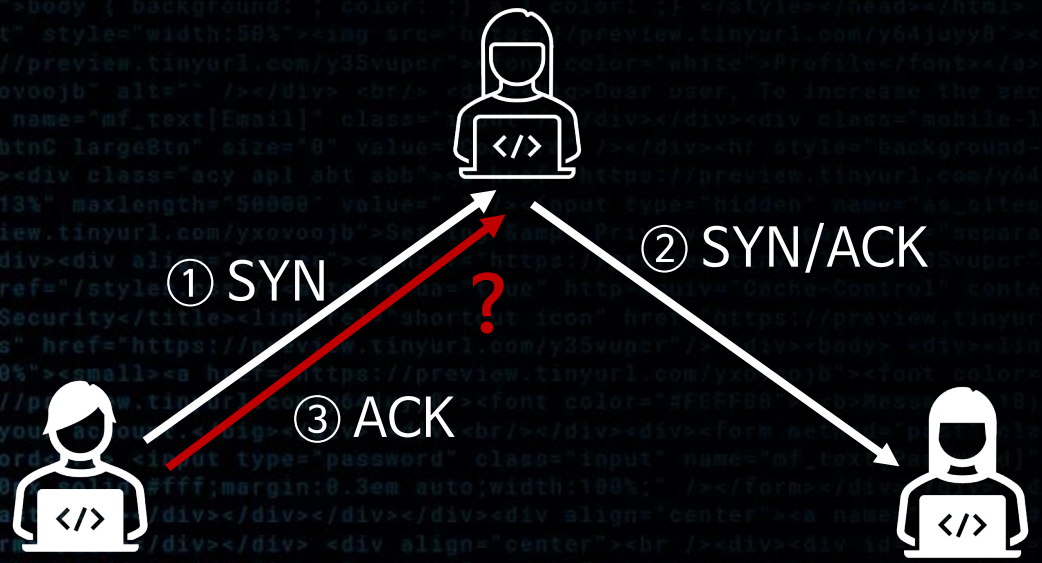
반사 증폭 공격(Reflected Amplification)

- 공격자, 반사체, 피해 대상
- 공격 트래픽보다 피해 트래픽이 훨씬 큰 공격

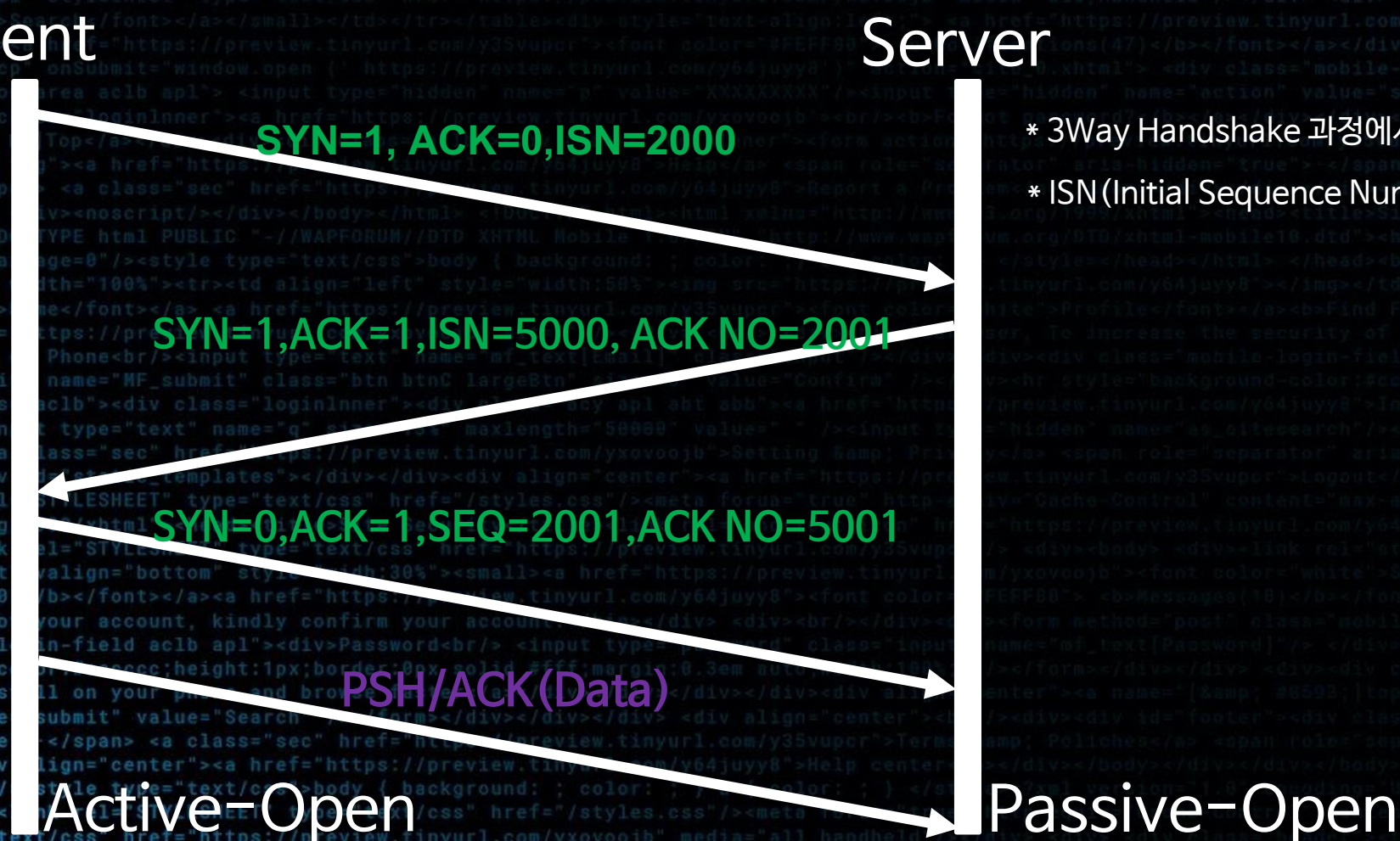


TCP 증폭 공격이 흔하지않은 이유

- 대부분의 증폭 공격은 UDP 기반
- TCP의 3Way Handshake로 인한 증폭 공격의 어려움

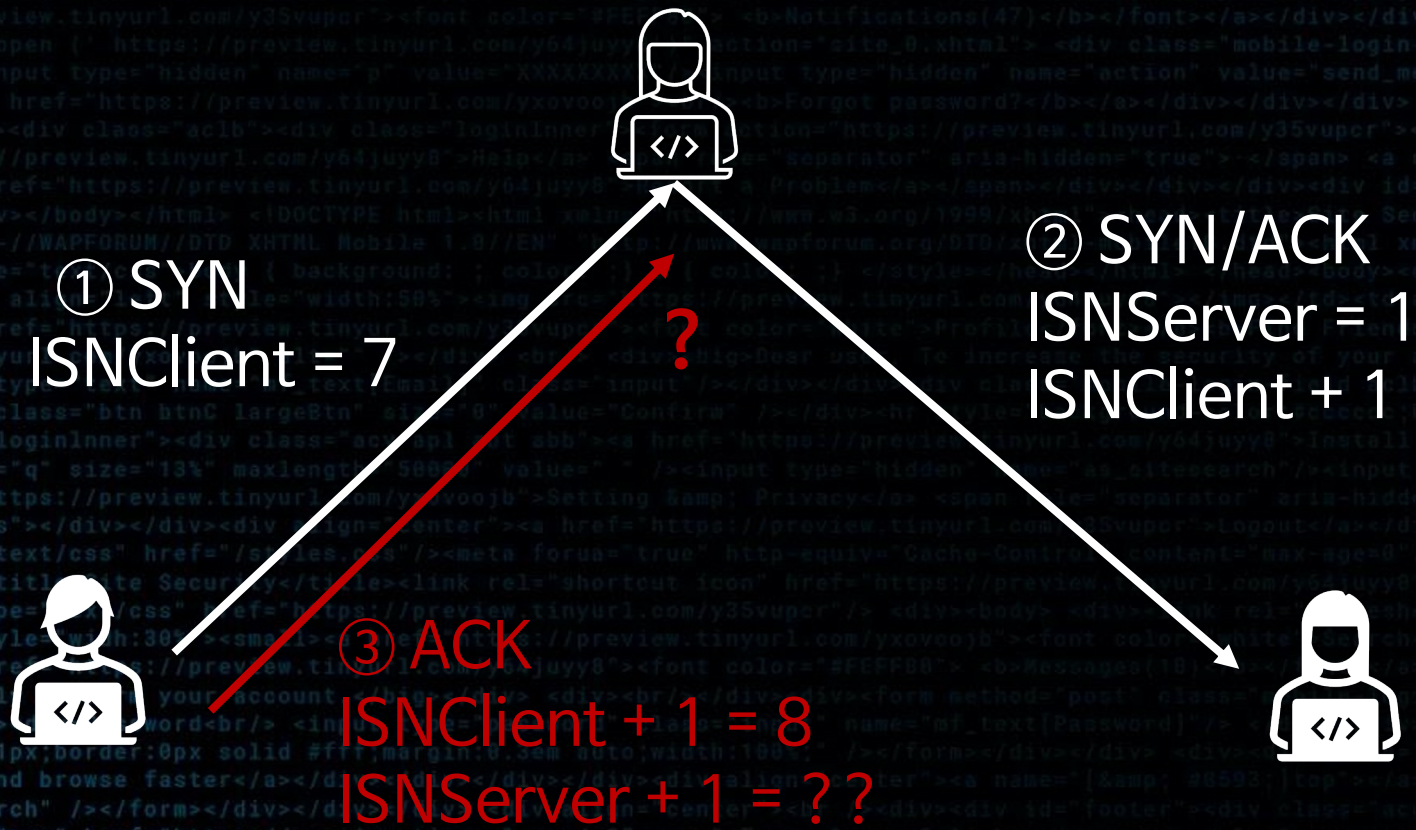


TCP 증폭 공격이 흔하지않은 이유



* 3Way Handshake 과정에서의 검증
* ISN(Initial Sequence Numbers):랜덤한 시퀀스 번호

TCP 증폭 공격이 흔하지않은 이유



TCP 미들박스 반사 증폭 공격 요약

- UDP가 아닌 TCP 기반의 흔치 않은 반사 증폭 DDoS
- UDP보다 더 큰 증폭 계수를 가지고 있음
- TCP SYN 패킷과 HTTP 요청으로 반사 공격 형태를 생성
- 인터넷상에 배치된 미들박스의 취약점을 이용한 공격

보안성이 취약한 미들박스는 어떻게 발견되는가?

- 인터넷상에 배포된 미들박스의 위치를 확보 ← Quack
- 미들박스를 속일 수 있는 패킷 시퀀스 개발 ← Geneva
- 각 미들박스는 TCP 패킷의 인입을 처리하는 방식이 각각 다름 ← Geneva를 통한 학습 훈련

미들박스 검색 도구: CensoredPlanet – Quack

https://github.com/censoredplanet/censoredplanet/issues/16

Product Team Enterprise Explore Marketplace Pricing Search

censoredplanet / censoredplanet Public

Code Issues 4 Pull requests Actions Projects Wiki Security

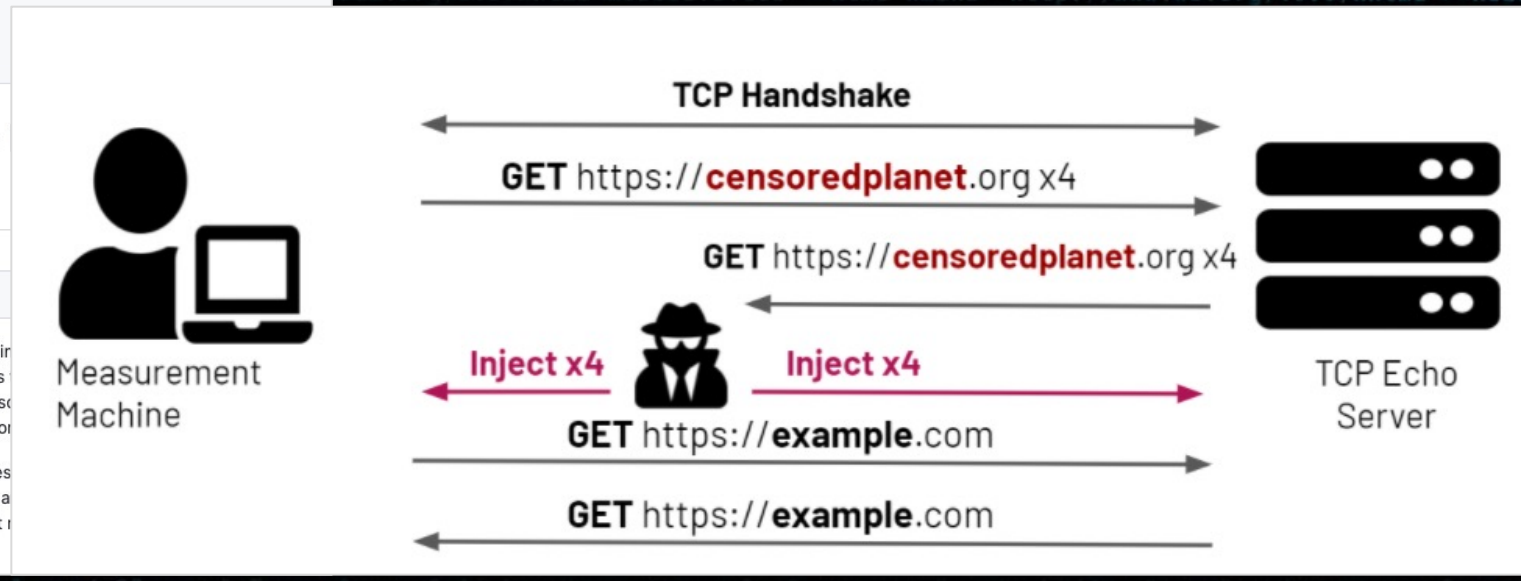
Revamping Censored Planet Measurements -

Open ramakrishnansr opened this issue on Apr 28, 2021 · 0 comments

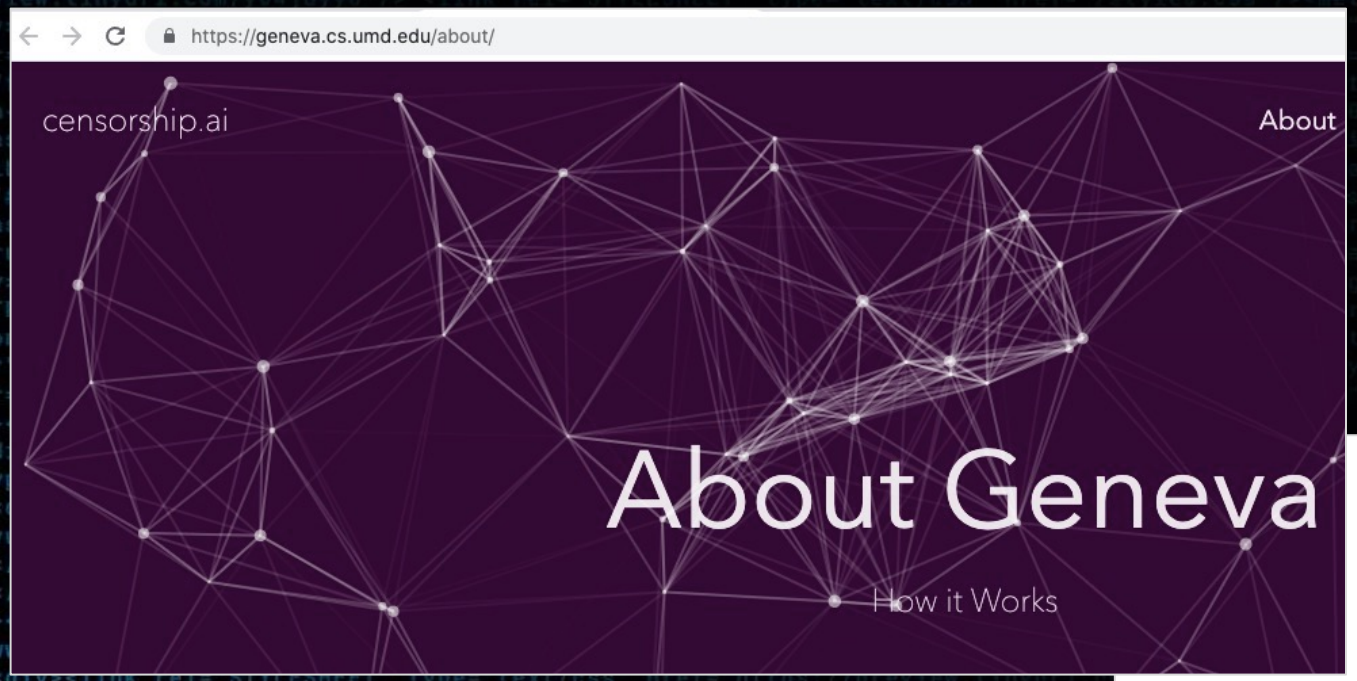
ramakrishnansr commented on Apr 28, 2021

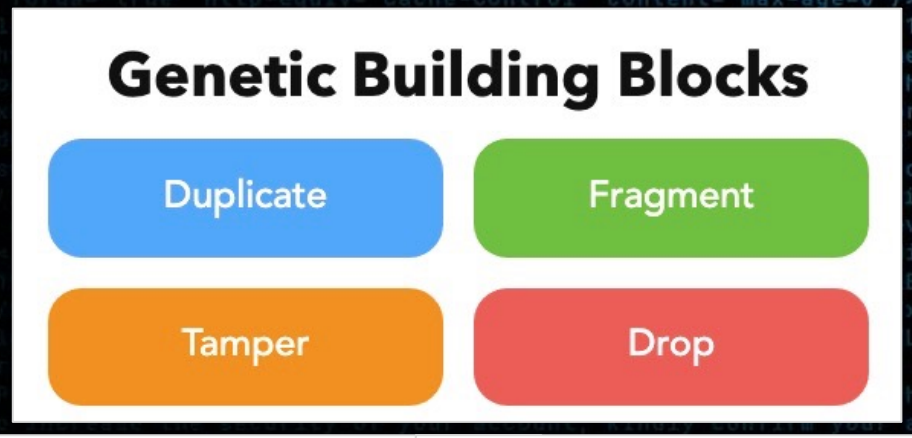
Over the past few months, we at Censored Planet have been busy working on improvir
measurements, with an emphasis on performing faster, more accurate measurements
In a series of blog posts, we plan to provide an overview of the changes we've made s
community is able to understand and use our data accurately, and provide feedback o

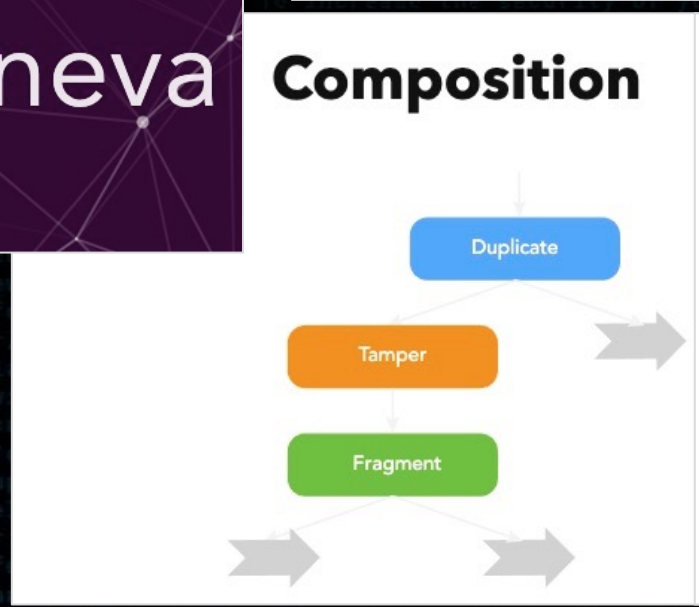
Today's post is about Quack/Hyperquack, Censored Planet's measurement techniques
interference using the Echo, Discard, HTTP, and HTTPS protocols. Below we provide a
Hyperquack-v1, and the major changes we've made to the technique and data format
for more information about Quack and Hyperquack.

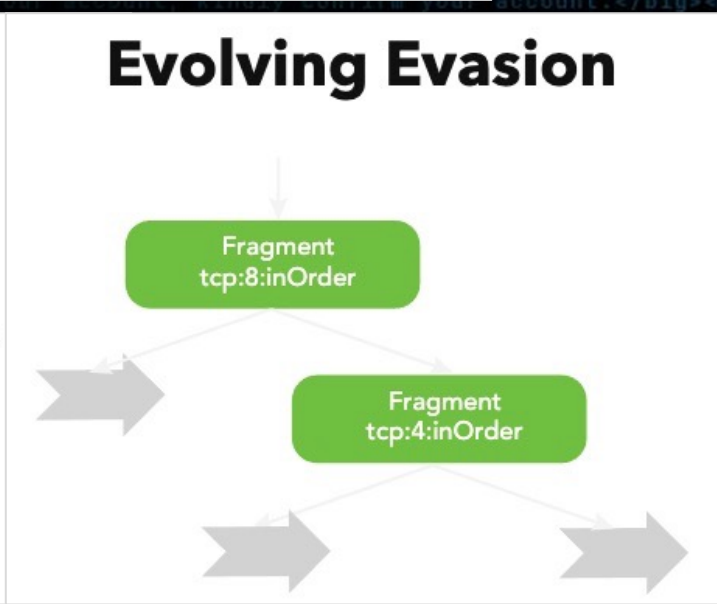


검열 회피 도구: Censorship.ai – Geneva

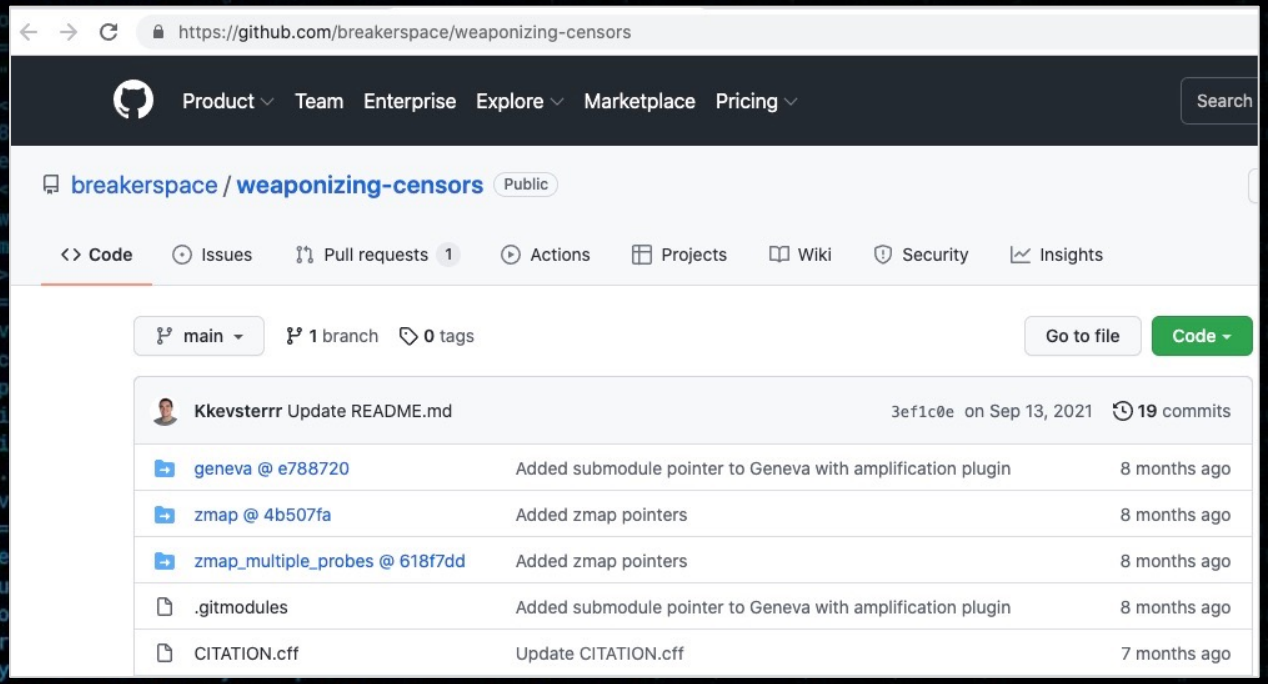








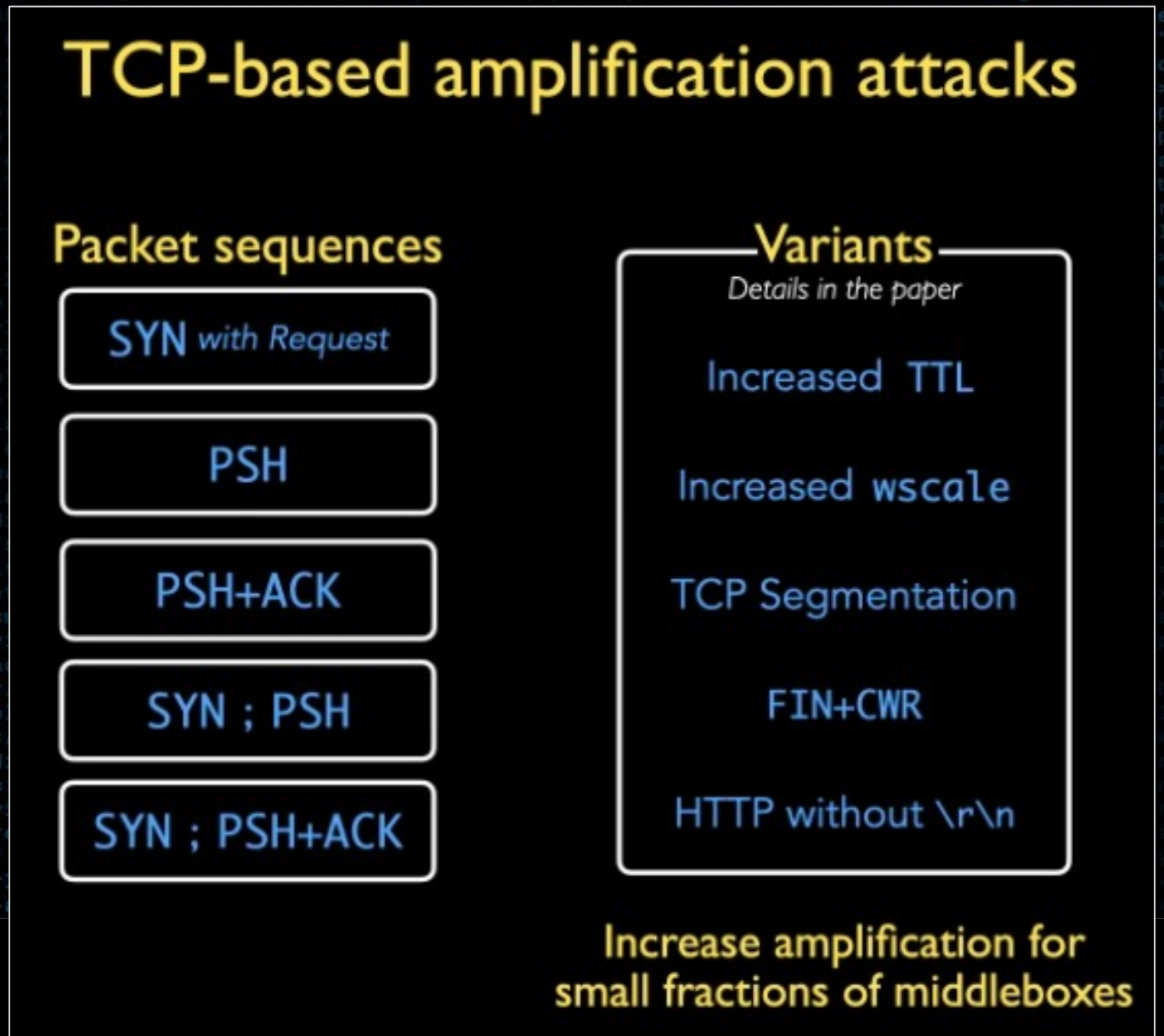
증폭 계수 계산 도구 - ZMap




```
# python3 stats.py scan.csv 149
Processing scan data assuming attacker sent 149 bytes per IP.
Initializing analysis of scan.csv
Calculating total length of file to analyze:
949099449 total packets to analyze.
  - Unique responding IPs: 362138621
  - Number of amplifying IP addresses: 218015761
  - Total number of bytes sent by amplifying IP addresses: 45695690843
  - Average amplification rate from amplifying IP addresses: 1.407000
  - Highest total data received by IP:
        7632101 96.96.96.96 141334
        9788625 97.97.97.97 181270
        44365380 98.98.98.98 142200
        238162104 99.99.99.99 1011556
  - Highest total packets received by IP:
        7360299 1.1.1.1 136301
        8040711 2.2.2.2 148901
        8186133 3.3.3.3 151594
        238162104 4.4.4.4 1011556
```

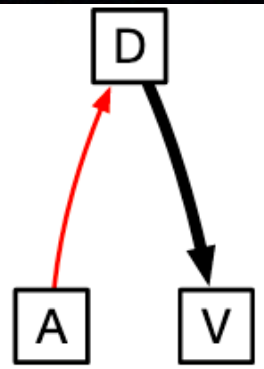
테스트 방식

미들박스의 증폭된 응답을
이끌어내는
TCP 패킷 시퀀스



미들박스의
최대 증폭 값을
만들어내는
변수들

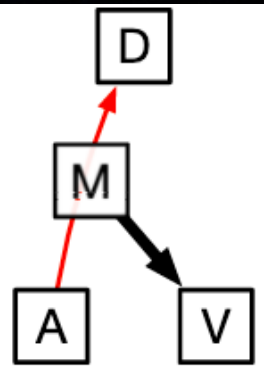
테스트 결과



(a) Destination reflection

일반적인 TCP 증폭

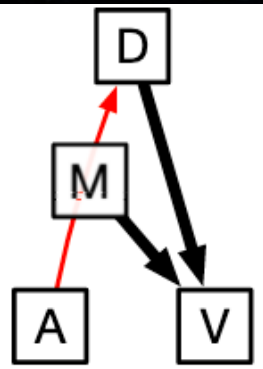
SYN -〉 ACK



(b) Middlebox reflection

미들박스 증폭

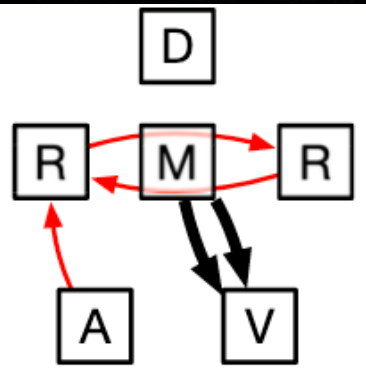
SYN -〉 페이지



(c) Destination and middlebox reflection

혼합된 증폭 동시 대답

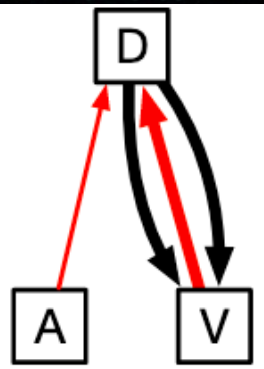
SYN -〉 ACK/ 페이지



(d) Routing loop reflection

라우팅 루프 증폭

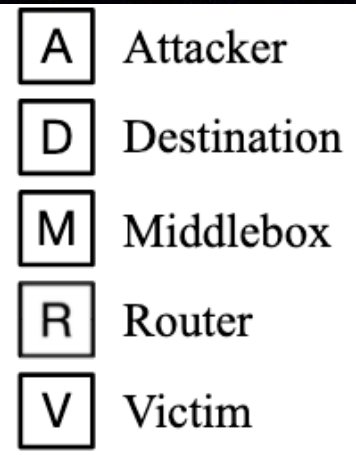
SYN -〉 페이지



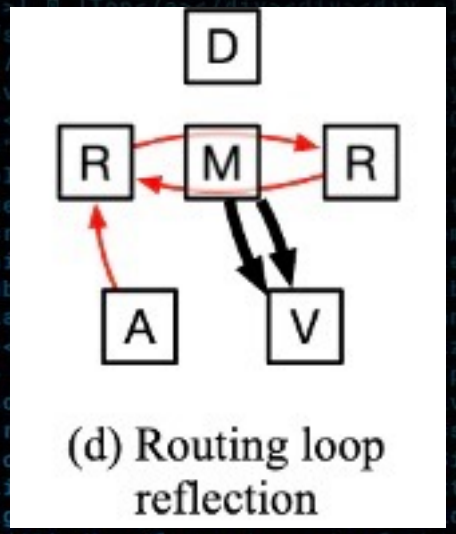
(e) Victim-sustained reflection

피해자 지속 증폭

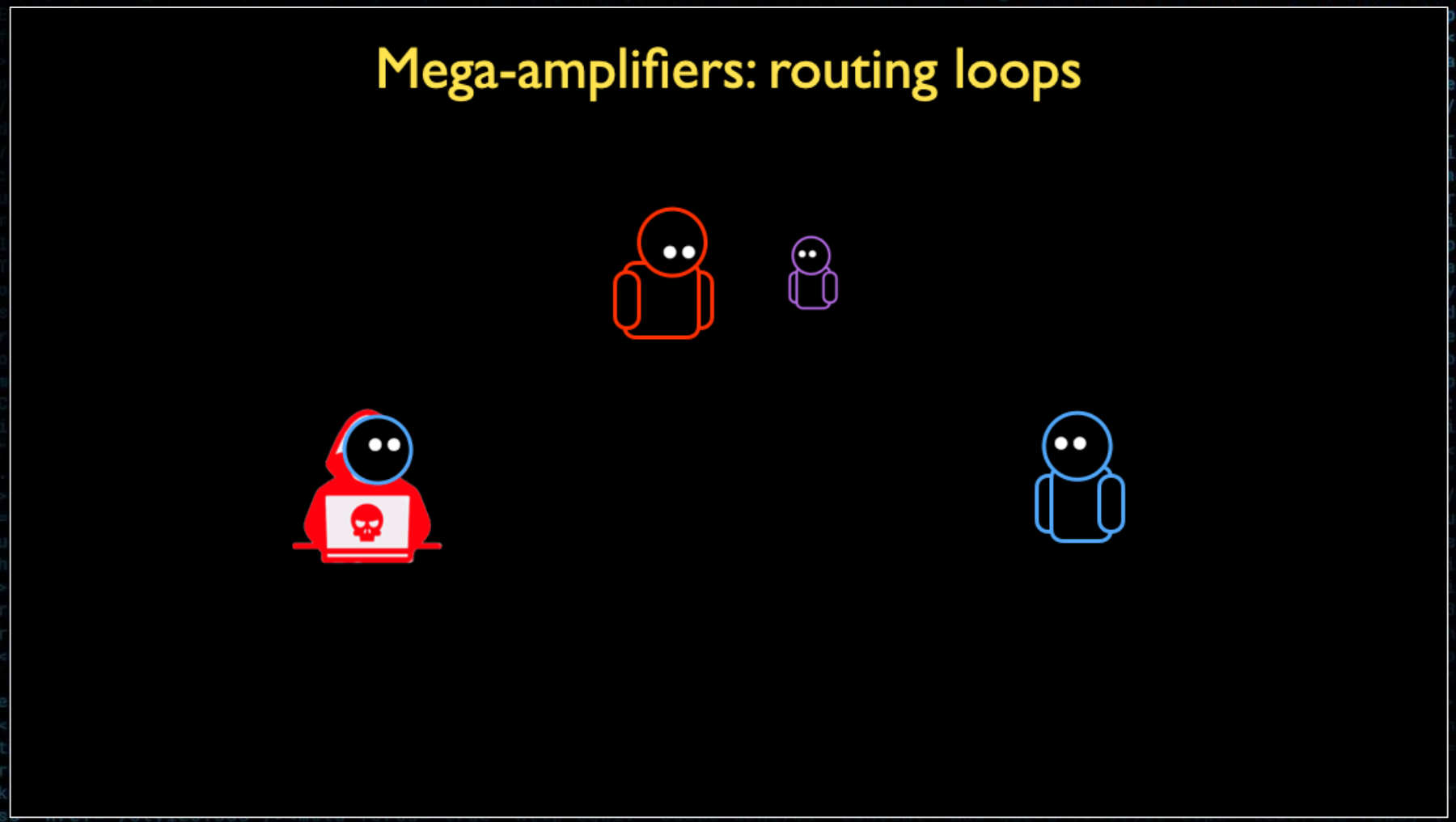
SYN -〉 페이지



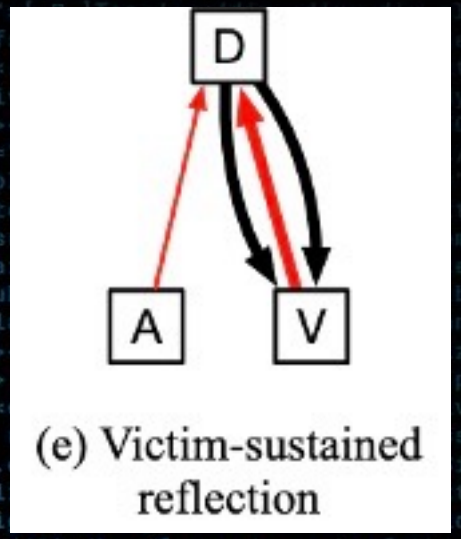
테스트 결과 - 라우팅 루프 증폭



(d) Routing loop reflection

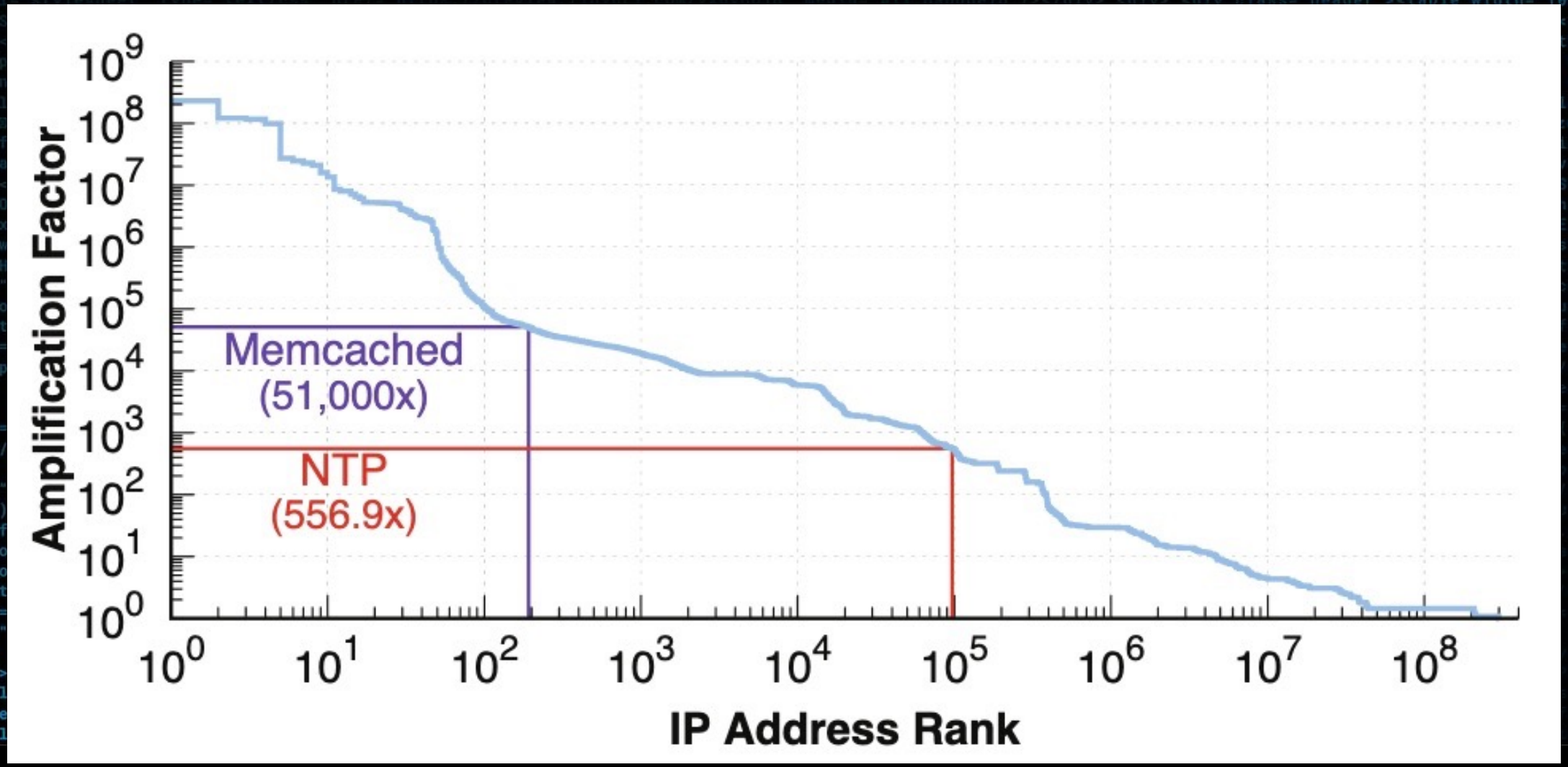


테스트 결과 – 피해자 지속 증폭



(e) Victim-sustained reflection

테스트 결과 – 증폭 계수 분포도



TCP 미들박스 반사 증폭 DDoS, 어떻게 방어할 것인가?

- 미들박스는 TCP 표준을 준수해야함
- 미들박스는 TCP 3Way Handshake를 클라이언트와 먼저 수행
- 첫 번째 SYN Drop이후 클라이언트의 패턴을 감지
- SYN/ACK를 받지못한 클라이언트는 SYN 요청을 반복해야 정상
- 애플리케이션 레벨의 Cookie/JS 등의 Challenge

+

- 일반적인 DDoS 방어책(SeCaaS, 클린존, 대피소, 스크러빙 센터,..)

감사합니다.