Middlebox Amplification 기법을 이용한 CAPTCHA 서버 기반 DoS 공격 분석

이혜진, 이웅희, 최경록, 허준범
고려대학교

{hjlee, whlee, krchoi, jbhur}@isslab.korea.ac.kr

Analysis of DoS Attack Using Middlebox Amplification on CAPTCHA Server

Lee, Hye Jin; Lee, Woong Hee; Choi, Kyung Rok; Hur, Junbeom
Korea Univ.

요 약

본 논문은 CAPTCHA 서버를 Middlebox 로 활용하여 보안 위협이 되는 Reflected Amplification DoS 공격 가능성을 이해함으로써 실증 및 분석을 하였다. 또한 CAPTCHA 서버의 응답 구조를 활용한 증폭 효과를 평가하고, 이를 기반으로 보안 설계상 취약점을 고찰하였다.

Ⅰ. 서론

서비스 거부 공격 (DoS)이란 시스템을 악의적으로 공격해 시스템의 리소스를 부족하게 하여 원래 의도된 용도로 사용하지 못 하게 하는 공격이다. DoS 공격자가 사용하는 주요 기술 중 하나는 트래픽을 증폭시키는 능력이다. 오늘날 DoS 공격은 인터넷 인프라에 심각한 위협 요소로 작용하고 있다. 최근 수년간 발생한 여러 대규모 DoS 공격 사례는 이러한 위협의 현실성을 잘 보여준다. 이와 같은 공격은 단순한 트래픽 유입을 넘어서, 기업 및 기관의 신뢰도 저하, 경제적 손실, 그리고 사이버 안보에 대한 우려로 이어지고 있다. 이에 따라 다양한 DoS 공격 기법과 방어 전략에 대한 연구가 활발히 이루어지고 있다. 기존에는 트래픽 기반 공격을 탐지하거나 필터링하는 네트워크 보안 기술이 주류를 이루었지만, 최근에는 증폭 및 반사 기법을 활용한 고도화된 공격들이 등장하면서, 중간자나 공개된 서비스를 악용하는 공격 시나리오에 대한 연구가 증가하고 있다. 이러한 맥락에서 CAPTCHA 인증 서버와 같은 인증 기반 시스템 역시 새로운 공격 벡터로 주목받고 있다.

본 연구에서는 이러한 흐름에 따라, Middlebox 로 활용될 가능성이 있는 CAPTCHA 서버를 대상으로, 증폭 공격의 가능성과 그 실현 가능성을 실험적으로 분석한다.

Ⅱ. 본론

2.1 배경지식

A. Middlebox 의 개념

Middlebox 는 클라이언트와 서버 간의 통신 경로 중간에 위치하여 네트워크 트래픽을 제어하거나 변환하는 장치를 통칭한다. Middlebox 는 방화벽, NAT, 프록시 서버, 로드 밸런서, IDS/IPS 등과 같이 다양한 기능을 수행하며 네트워크 보안 및 성능 개선을 목적으로 사용된다. 최근에는 특정 응답을 대신 처리하거나 필터링하는 기능을 가진 인증 서버나 API 게이트웨이도 넓은 의미에서 Middlebox 의 범주에 포함되고 있다. 이러한 장치는 응답을 자동으로 생성하거나 전달하는 특성으로 인해, 공격자가 이를 악용하여 증폭 및 반사 공격에 이용할 수 있다.

B. Reflection 및 Amplification 공격

Reflection 공격은 공격자가 요청자를 위조하여, 제 3 의 서버(Middlebox 등)로 요청을 보냄으로써 해당 서버가 피해자에게 직접 응답을 보내도록 유도하는 방식이다. 또한, Amplification 공격은 요청 대비 훨씬 큰 크기의 응답이 발생하도록 유도하여, 적은 자원으로도 막대한 트래픽을 생성할 수 있게 한다. 이 두 방식은 종종 함께 사용되며, Reflected amplification DoS 공격을 일으킬 수 있다. CAPTCHA 서버가 자동 응답 기능과 상대적으로 큰 응답 패킷을 생성하는 구조를 가지고 있다는 점에서, 이러한 CAPTCHA 서버가 공격에 사용될 가능성이 있다. 특히, HTTP 기반으로 동작하는 CAPTCHA 서버의 경우, 요청 헤더 조작을 통해 응답의 크기를 인위적으로 증가시킬 수 있는 여지가 존재한다. 이러한 가능성은 본 연구의 실험을 통해 분석 대상이 된다

C. CAPTCHA 서버와 Proof-of-Work 메커니즘

CAPTCHA 는 웹 서비스에서 자동화된 봇의 접근을 방지하기 위해 널리 사용되는 인증 방식이다. 최근에는 전통적인 이미지 식별, 문자 인식 등 전통적인 CAPTCHA 외에도, 계산 자원을 소모하게 하는 Proof-of-Work (PoW) 기반 인증 메커니즘이 등장하고 있으며, 이는 사용자가 서비스 제공자에게 특정 계산 노력의 일정량이 소모되었음을 증명하는 암호화 증명 의 한 형태다. 대표적인 PoW 기반 상용 CAPTCHA 서버로는

Google reCAPTCHA, Cloudflare Captcha 등이 있으며, 오픈소스 CAPTCHA 서버로는 mCaptcha[2], ALTCHA, CAP 등이 있다. 이러한 서버는 특정 요청에 대해 PoW 과제를 포함한 응답을 자동으로 생성하여 전달하게 되며, 이로 인해 적절한 조건이 갖추어질 경우 DoS 공격에서 Middlebox 로 활용될 여지가 있다.

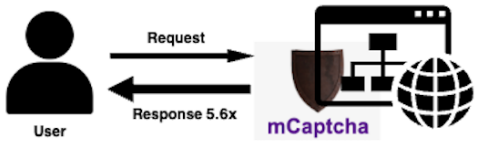

Fig.1 Normal Workflow

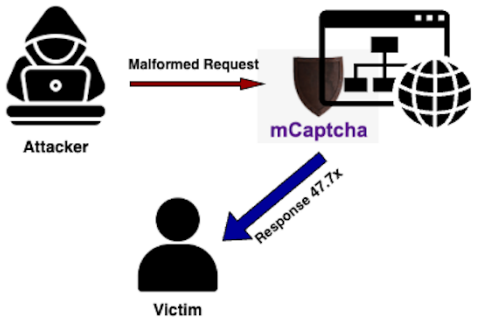

Fig.2 Attack Workflow

2.2. 실험

A. 실험 대상 및 환경 구축

본 연구에서는 PoW 메커니즘을 사용하는 오픈소스 CAPTCHA 서버 중 하나인 mCaptcha 를 실험 대상으로 선정하였다. 해당 구조는 ALTCHA, CAP 등 다른 CAPTCHA 시스템과 기술적으로 유사하여, 본 실험 결과의 일반화 가능성이 높다고 판단하였다.

실험 환경은 로컬 네트워크 상에서 구성되었으며, mCaptcha 서버를 직접 설치 및 구성하여 테스트를 진행하였다. 모든 실험은 동일한 네트워크 조건에서 이루어졌으며, 외부 요인에 의한 변수를 최소화하였다.

B. 실험 목적 및 접근 방식

본 실험의 목적은 CAPTCHA 서버가 트래픽 증폭에 얼마나 취약한지를 확인하는 것이다. 특히 본 연구에서는 IP spoofing 기법에 집중 하기 보다는, CAPTCHA 서비스의 구조적 특성이 증폭 공격에 이용될 수 있는지를 중점적으로 분석하였다. 따라서 CAPTCHA 서버를 amplification 공격의 middlebox 로 사용할 수 있는 가능성에 초점을 두었다.

C. 실험 방법

HTTP 헤더 정보를 조작하는 방법을 사용하여 요청을 생성하였고, 이를 통해 서버가 더 큰 응답을 생성하도록 유도하였다. 정상 요청과 조작된 요청의 응답에 대한 Amplification Factor(AF)를 비교하여 해당 서버가 amplification 공격에 대해 효과적인 middlebox 인지 확인하였다.

{AF = 요청 패킷 크기/응답 패킷 크기}

2.3. 결과 및 평가

정상적인 HTTP 요청에 대한 총 요청 크기의 합은 5017 bytes, 총 응답 크기는 28227 bytes 로 측정되었다. 이를 바탕으로 계산한 증폭 계수(AF)는 5.6x 과 같다. [Fig.1]

반면, 조작된 요청의 크기는 305 bytes, 응답의 크기는 14536 bytes 로 증폭 계수는 47.7x 과 같다. [Fig.2]

이 결과, 정상 요청보다 작은 요청 크기로 훨씬 큰 응답을 받는 것을 확인하였다. 이는 CAPTCHA 서버가 단순 요청 변조만으로도 높은 증폭을 유발할 수 있음을 보여주며, IP spoofing 과 결합될 경우 실제 DoS 또는 DDoS 공격에 악용될 수 있는 middlebox 임을 알 수 있다.

Ⅲ. 결론

본 논문에서는 PoW 기반의 CAPTCHA 서버가 Reflected Amplification DoS 공격에 악용될 수 있는 가능성을 실험적으로 분석하였다. 실험 결과 CAPTCHA 서버가 단순한 요청 조작만으로도 증폭 공격에 효과적인 middlebox 로 사용될 수 있음을 의미한다. 이러한 결과는 CAPTCHA 서버가 인증 기능 외에도 네트워크 공격에 활용될 수 있음을 시사하며, 향후 CAPTCHA 시스템 설계 시 요청-응답 크기 비율에 대한 제약, 정책의 강화, 비정상적인 요청 필터링 등의 보안 강화 방안이 요구된다.

우리는 다양한 상용 CAPTCHA 시스템에 대한 후속 실증 연구와, 실 네트워크 환경에서의 amplification 적용 가능성에 대한 분석을 진행할 예정이다. 우선 TCP handshake 가 가능하도록 IP spoofing 을 통한 실제 공격 적용 가능 여부에 대해 실험할 예정이다. 또한, [1]에서의 방식처럼 TCP 패킷 payload 에 HTTP 요청을 실어 보내도록 조작하여 TCP handshake 를 완료하지 않고도 요청을 받아들이도록 할 수 있는지 실험할 예정이다. 서버가 요청을 받아들이게 되면 실험 결과와 같이 실제 amplification 을 유도할 수 있다. 이러한 후속 연구를 통해 우리는 CAPTCHA 를 활용한 공격 범위를 확장할 예정이다.

ACKNOWLEDGMENT

이 논문은 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원-대학 ICT 연구센터(ITRC)의 지원(RS-2021-II211810)과 한국연구재단의 지원을 받아 수행된 연구임(RS-2025-00563143, RS-2021-NR060143).

참 고 문 헌

[1] Kevin Bock, Abdulrahman Alaraj, Yair Fax, Kyle Hurley, Eric Wustrow, and Dave Levin. Weaponizing middleboxes for TCP reflected amplification. In Proceedings of the USENIX Security Symposium, 2021.

[2] mCaptcha. https://github.com/mCaptcha

[3] Pan, Y. and Rossow, C. TCP spoofing: Reliable payload transmission past the spoofed TCP handshake. In Proceedings of 2024 IEEE Symposium on Security and Privacy, 2024.

[4] Daniel Wagner et al. United We Stand: Collaborative Detection and Mitigation of Amplification DDoS Attacks at Scale. In CCS. ACM, 2021.