DNS-based DDoS Mitigation Solution

MMLAB: 양석훈, 선민준, 전진용

2023 Spring Creative Integrated Design 2 Final Presentation

Abstract

- Target server는 분산된 공격자에 일일이 대응하기 어렵지만, DNS server는 자신 영역의 attacker들을 관리하기 편함
- Puzzle을 통해 DDoS를 방어하는 서비스는 이론적 제안에 그침
  => DNS server와 Target server가 협력하여 Puzzle을 사용하는 DDoS mitigation solution 구축

1. Approach

DNS	Target server가 분산된 공격자에 대응하기 어려움 반면, Local DNS의 경우 자신의 영역만 관리하면 됨
Puzzle	사용자가 서버와 통신하기 앞서 문제를 풀어야 함 Puzzle을 이용해 rate limiting을 할 수 있음

Local DNS와 Target server가 협력하는 시스템 구축

- DNS server가 사용자에게 puzzle을 출제함
- 사용자는 서버에 접근하기 위하여 puzzle을 해결함
- Target server는 유효한 query에 대해서만 응답함

2. Goal

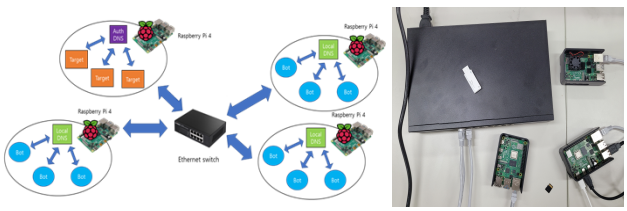
Kernel level에서 puzzle system 구현

- 유의미한 서버 부하 감소가 있어야 함
- 기존 통신 구조를 바꾸지 않아야 함 (User level 변화 최소)
- 실시간으로 정책을 수정할 수 있으며 DNS마다 개별적인 정책을 적용할 수 있어야 함

Target server의 부하를 기준으로 평가함

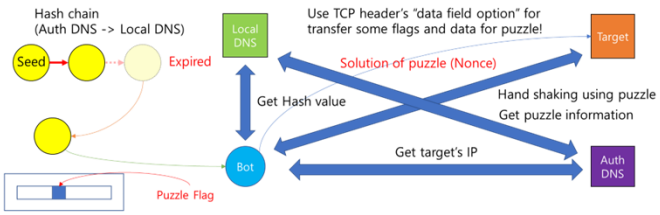
- 대조군(기존): Target server가 puzzle을 제공하는 경우
- 실험군(제안): Local DNS가 puzzle을 제공하는 경우
- 10배의 개선을 목표로 함

3. Implementation

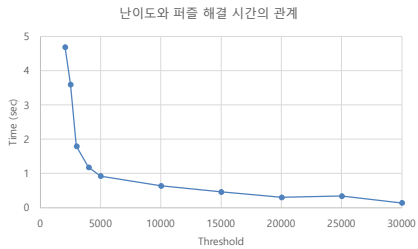


- **리눅스 커널의 통신 과정을 수정해 퍼즐 시스템을 구현**
  - 기존 리눅스 커널의 통신 구현체들을 수정 및 새로운 과정을 생성
  - **TCP와 UDP 통신 과정을 구현하여 server와 DNS resolver를 제작**
  - User level에서는 puzzle에 대한 고려가 필요 없음
  - OS에 무관한 하위호환성을 가지며 기존 코드 활용했기 때문에 이식성 가짐
  - 시스템 콜을 이용하여 puzzle 정책을 실시간으로 조절할 수 있음
  - Puzzle의 경우 Hash function을 활용하였기에 랜덤성 및 재사용 방지 가능

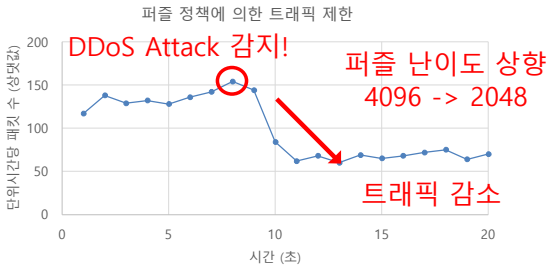
- **자체적으로 test bed를 구축**
  - **Raspberry Pi가 4코어임을 이용**
  - 3개의 Raspberry pi는 사용자를 구현하는 데 사용
  - 각각의 address block에는 3개의 공격자와 하나의 local DNS를 포함
  - 나머지 1개는 target server와 auth DNS를 구현하는 데 사용
  - 서버는 3코어로 구현하였고 auth DNS에 나머지 1개의 코어를 할당
  - 전체 4개의 Rasbpberry pi를 1Gb ethernet switch에 연결



4. Result



- Hash(Nonce, Souce IP, DNS IP, Token hash) ≤ Threshold
- Threshold를 낮출수록 적당한 Nonce를 찾기 어려워짐
- Threshold를 낮추면 퍼즐 해결 시간이 증가함을 확인함



- 외부에 영향을 주지 않기 위해 in house로 실험하였음
- Puzzle을 사용하지 않는 경우, 패킷 수 증가시 server에 가해지는 부하 급증
- Target server가 공격을 감지하여 퍼즐의 난이도를 상향한 결과 트래픽이 감소하였음
- 퍼즐 시스템이 정상적으로 작동함을 확인하였음
- DDoS 평가시 연결 실패하는 경우 존재하지 않음

4. Conclusion and Future Work

- 제안한 puzzle system을 Raspberry Pi 상에서 실험함
- Puzzle은 기대한 대로 능동적인 rate limiting을 수행함
- Puzzle과 DNS를 사용함으로써 server의 부하가 감소
- Puzzle 정책 개선을 통한 성능 개선이 가능함을 확인함

- 로컬에서 테스트 완료
- 다양한 상황에 대해 테스트하여 효과적인 puzzle 정책을 찾아낼 예정

5. References

1. Ali, Isra Mohamed, Maurantonio Caprolu, and Roberto Di Pietro. "Foundations, properties, and security applications of puzzles: a survey." ACM Computing Surveys (CSUR) 53.4 (2020): 1-38.
2. Abraham, Anup Mathew, and Shweta Vincent. "Defending DoS Attacks Using a Puzzle-Based Approach and Reduction in Traceback Time towards the Attacker." Global Trends in Computing and Communication Systems: 4th International Conference, ObCom 2011, Vellore, TN, India, December 9-11, 2011. Proceedings, Part I. Springer Berlin Heidelberg, 2012.
3. Feng, Wu-chi, Edward Kaiser, and Antoine Luu. "Design and implementation of network puzzles." Proceedings IEEE 24th Annual Joint Conference of the IEEE Computer and Communications Societies.. Vol. 4. IEEE, 2005.
4. Abliz, Mehmud, and Taieb Znati. "A guided tour puzzle for denial of service prevention." 2009 Annual Computer Security Applications Conference. IEEE, 2009.