클라우드 컴퓨팅 공격 및 방어 플랫폼 개발

YoYo Attack에 특화된 방어 플랫폼

분과 C 32 [DDALPI] 팀
이강빈 장진영 강수민

목차

Part 1,

배경설명 및 목표

Part 1,

배경설명 및 목표

과제 배경

클라우드의 확대

클라우드 서비스 사용이 전세계적인 증가로 인해, 많은 사람들이 클라우드에 관심을 갖게 되었고,
해커들 또한 클라우드 환경에 주목하게 되었다.

취약점 발견

클라우드 환경에 특화된 EDoS 와 같은 공격들이 생겨났다. YoYo Attack은 클라우드 과금 방식의 취약점을 노리는 새로운 공격방식이다.

새로운 방어 매커니즘

전통적인 DDoS의 방어 방식으로는 YoYo Attack과 같은 EDoS를 방어하는데 한계가 있어 새로운 방어 매커니즘이 필요하다.

Part 1,

배경설명 및 목표

YoYo Attack 이란??

YoYo Attack이 뭐야? => Application Layer 공격을 이용한 서버 과금 유도

공격 중단 | 공격 | 공격 중단 | 공격 | 공격 중단

공격자

서버

배경설명 및 목표

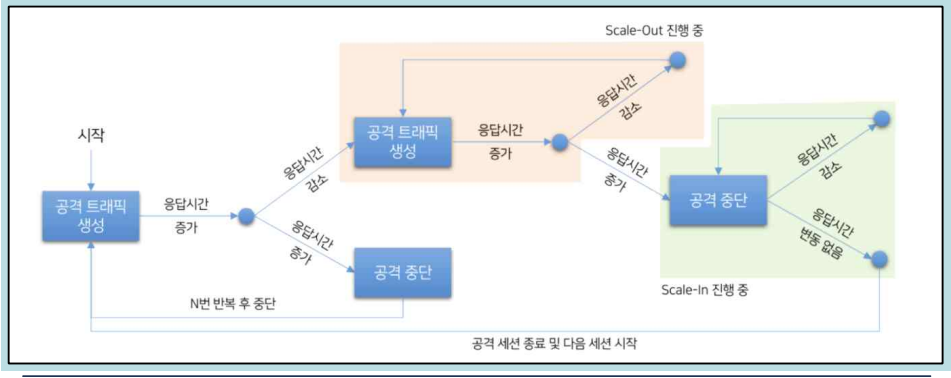
목표

1. 클라우드 환경에서의 자원 자동 확장 기능을 악용한 YoYo Attack 공격을 감지하고,
   이를 방어할 수 있는 실시간 알고리즘을 개발한다.
2. YoYo Attack에 특화된 공격 매커니즘을 개발한다.
3. 공격자의 공격 성공 여부에 대한 판단에 혼란을 야기하고,
   서버의 자원 관리와 비용 효율성을 동시에 보장할 수 있는 방어 매커니즘을 개발한다.
4. 공격자, 서버(방어자) 대시보드를 개발한다.

배경설명 및 목표

제안하는 공격 및 방어 매커니즘

제안하는 공격자 매커니즘



공격자 입장에서 공격 매커니즘

배경설명 및 목표

서버(방어자) 목표

다수의 정상 사용자

서비스를 이용하는 정상 사용자
서비스의 대부분의 이용자로
정상사용자는 서비스 이용에 있어서
불편함을 느껴선 안된다.

공격자 의심 사용자

서버가 갖는 내부 정보를 통해 색출
공격자가 IP를 바꾸거나 분산해서 공격하여도
엔지니어가 알고 있는 서버 내부의 데이터를
통해서 공격자의 수와 IP변경에 상관없이
공격자로 의심되는 사용자를 색출 가능하다

다수의 정상 사용자들은 방어 매커니즘이 설정된 서버 환경에서도 정상적인 서비스를 이용하되
공격자로 의심 되는 IP에 대해서는 방어 매커니즘을 통해 공격을 방어해야한다.

어떻게? => 공격자의 **응답 시간**을 교란 한다.

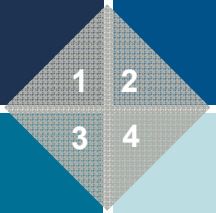
배경설명 및 목표

제안하는 공격 및 방어 매커니즘

제안하는 방어자 매커니즘

- 특정 IP Sleep
  단위시간 당 요청 횟수에 따라
  해당 IP를 처리하는 스레드에 Sleep

- VM 방화벽 설정을 통한 패킷 드랍
  단위시간 당 요청횟수에 따라
  방화벽 설정을 통해 일정시간 패킷 드랍



- 더미 서버 기반의 확률적 리다이렉트
  단위시간 당 요청 횟수에 따라
  해당 IP를 더미서버로 리다이렉트

- OpenWRT 를 활용한 중개방어
  단위시간 당 요청횟수에 따라
  OpenWRT가 설치된 공유기에서 응답지연

Part 2,

실험 구성

Part 2,

실험 구성

전체적인 시스템 구성 및 다이어그램

도커

컨테이너 이미지를 기반으로
웹 어플리케이션을 배포

쿠버네티스

컨테이너화 된 어플리케이션 리소스
사용률에 따라 Auto Scaling

그라파나

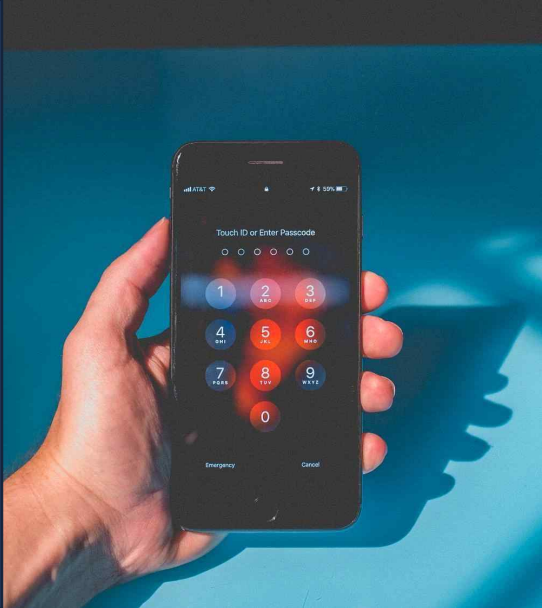
웹 어플리케이션의 상태와 성능 지표
수집 및 시각화 도구

스프링부트

공격자와 방어자가 사용하는
웹 대시보드 개발에 활용

Part 3,

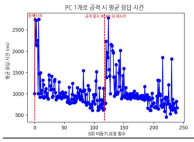
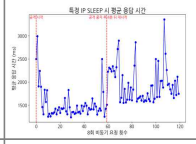
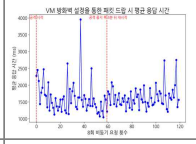
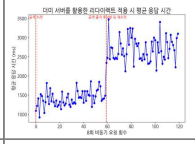
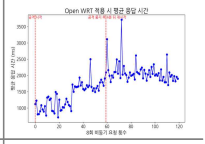
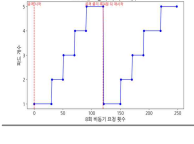
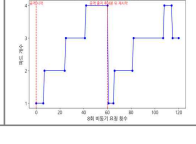
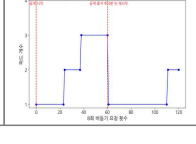
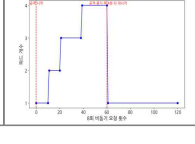
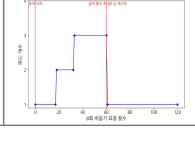
실험 결과


AT&T
53%
Touch ID or Enter Passcode
1
2 ABC
3 DEF
4 GHI
5 JKL
6 MNO
7 PQRS
8 TUV
9 WXYZ
0
Emergency
Cancel

Part 2,

실험 결과

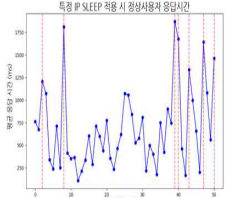
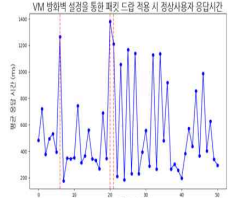
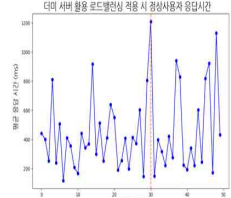
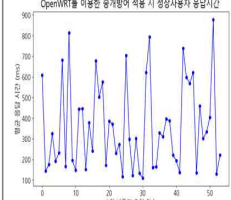
제안하는 방어 매커니즘

공격자 실험 결과 (방어 시스템이 없을 때)	특정 IP Sleep	VM 방화벽을 통한 확률적 패킷 드랍	더미 서버 기반의 확률적 리다이렉트	OpenWRT를 이용한 중개 방어
				
				

Part 2,

실험 결과

방어 매커니즘으로 인해 정상사용자가 피해를 입는가?

특정 IP Sleep	VM 방화벽을 통한 확률적 패킷 드랍	더미 서버 기반의 확률적 리다이렉트	OpenWRT를 이용한 중개 방어
			
서비스의 불편을 느끼는 응답 시간 (1200ms 이상) : 7회 관측 평균 응답시간: 687.0 ms	서비스의 불편을 느끼는 응답 시간 (1200ms 이상) : 3회 관측 평균 응답시간: 543.0 ms	서비스의 불편을 느끼는 응답 시간 (1200ms 이상): 1회 관측 평균 응답시간: 442.0 ms	서비스의 불편을 느끼는 응답 시간 (1200ms 이상): 0회 관측 평균 응답시간: 359.0 ms

감사합니다!