트래픽 폭주 공격의 탐지를 위한 패킷 분석

Packet Analysis for Detecting Traffic Flooding Attack

원승영*, 구향옥*, 구경옥**, 오창석*
충북대학교*, 강릉영동대학**

Won Seung-Young*, Koo Hyang-Ohk*,
Koo Kyung-Ok**, Oh Chang-Suk*
Chungbuk National Univ.*,
Gangneung Yeongdong College**

요약

트래픽 폭주 공격은 네트워크 대역폭, 프로세스 처리 능력, 기타 시스템 자원을 고갈시킴으로써 정상적인 서비스를 할 수 없도록 하는 공격형태이며, 네트워크가 느려지거나 접속 불능 상태 등으로 인지할 수도 있지만 트래픽 폭주를 발생시킨 패킷을 수집하고 분석하는 방법을 이용하면 보다 정확한 공격의 탐지가 가능하다. 본 논문에서는 트래픽 폭주 공격을 보다 정확하게 탐지할 수 있도록 패킷 분석 기법을 제안하였다.

Abstract

A traffic flooding attack is an attack type that interfere with normal service by running out network bandwidth, process throughput, and system resource. It can be recognized intuitively by network slowdown, connect impossibility state and detected more exactly by collecting and analyzing packets that generate traffic flooding. In this paper, the packet analysis scheme is proposed for the more precise detection.

I. 서론

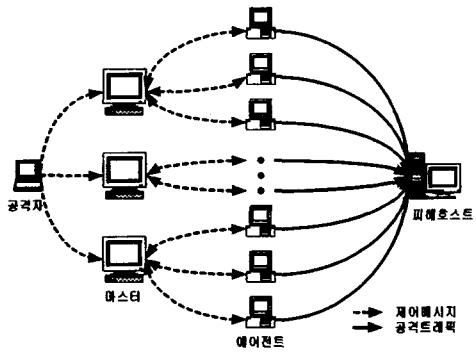
최근 인터넷 보안 체계를 공격하는 경향은 네트워크 자원 및 시스템을 공격 대상으로 사용 가능한 자원을 모두 소비해서 실제 자원을 사용해야 하는 사용자가 자원을 사용할 수 없게 하는 트래픽 폭주 공격이 주를 이루고 있다. 그 중에서도 서비스 거부 공격이 증가하고 있는 실정이다. 또한 다수의 시스템에 공격 에이전트를 설치 후, 동시에 공격함으로써 엄청난 파괴력을 지닌 분산 서비스 거부 공격도 일반화되는 추세이다.[1] 트래픽 폭주 공격의 인지는 시스템이나 네트워크가 느려지거나 접속 불능 상태 또는 cpu, 메모리 사용량 등을 통해 직관적으로 인지할 수 도 있지만 보다 정확하고 계량적인 분석을 통한 트래픽 폭주 공격의 탐지가 필요하다. 현재 침입 탐지에 대한 연구는 활발히 진행되고 있으며 상용화된 침입 탐지 시스템들도 개발되어 사용하고 있다. 하지만 트래픽 폭주 공격의 심각성에 비해 트래픽 폭주 공격에 대한 탐지 및 대응에 관한 연구는 관련 대학과 연구소에서 진행 중에 있지만 아직 미흡한 실정이다. 트래픽 폭주 공격의 탐지에 있어서 가장 중요한 부분은 공격을 정확히 탐지하는 것이다. 트래픽 폭주가 발생하였다고 하여 모두 공격으로 탐지하고 대응조치를 한다면 인터넷 사용자와 공급자 모두에게 크나큰 손실을 가져오게 될 것이다. 따라서 본 논문에서는 트래픽 폭주를 발생시킨 패킷을 수집하고 근원지 ip 주소와 목적지 포트번호, 프로토콜 등 공격 트래픽의 특징을 분석할 수 있도록 패킷을 분석하여 공격 트래픽을 탐지하였다.

II. 관련연구

1. DDoS 공격

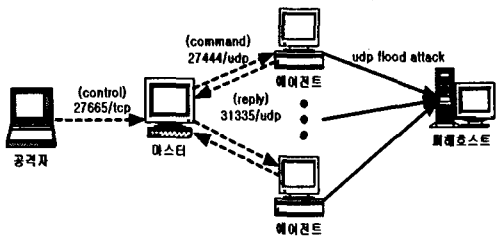
트래픽 폭주 공격의 대표적인 DDoS 공격은 여러 에이전트를 이용하여 동시에 피해호스트로 DoS 공격을 행함으로써 일반적인 DoS 공격보다 강력한 파괴력을 가지고 있다. DDoS의 일반적인 공격 방법은 공격자가 취약한 호스트를 해킹하여 사용권한을 얻은 마스터를

제어하고 마스터는 에이전트로 하여금 엄청난 패킷이 피해호스트로 전송됨으로써 피해호스트는 정상적인 서비스를 하지 못하게 되는 것이다. 그림 1은 DDoS 공격의 기본 구조이다.[2]



▶▶ 그림 1. DDoS 공격의 기본 구조

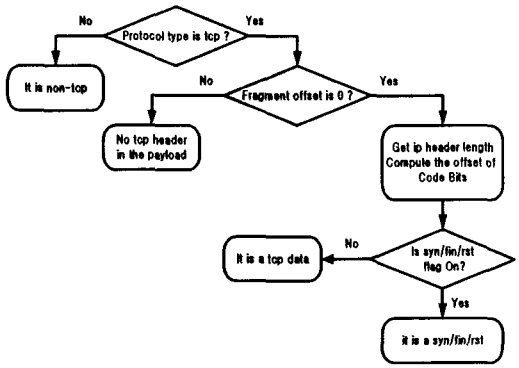
트래픽 폭주 공격의 종류 중 DDoS 공격의 대표적인 공격 도구로서 trin00는 udp flooding 공격을 위해 사용되는 도구이다. 공격의 몇 개의 마스터와 수많은 에이전트로 구성된다. 그림 2는 trin00 공격의 구조이다. 공격자는 마스터를 tcp 포트 27665번을 이용하여 제어하고 마스터와 에이전트간의 통신은 udp 포트 27444번과 31335번을 이용하는 것이 trin00의 특징이다.[3] 이렇게 공격자는 마스터를 제어하고 에이전트를 이용하여 피해호스트에 udp flooding 공격을 함으로써 피해호스트로 하여금 서비스거부 상태를 만들게 된다. 피해호스트로 전송되는 트래픽의 근원지 ip 주소는 스프핑된 ip 주소를 사용하기 위하여 무작위로 생성된 근원지 ip 주소를 가지고 전송되며 목적지 포트번호인 udp 포트 번호 또한 무작위성을 갖는 것이 특징이다.



▶▶ 그림 2. trin00 공격의 구조

2. DDoS 공격의 탐지

Michigan 대학의 Hainig W.와 Danlu Z., Kang G. Shin은 tcp 헤더의 flag 비트의 syn, fin, rst를 이용하여 tcp syn flooding 공격을 탐지하는 연구를 하였다.[4] 그림 3은 tcp 패킷 분류 과정이다.

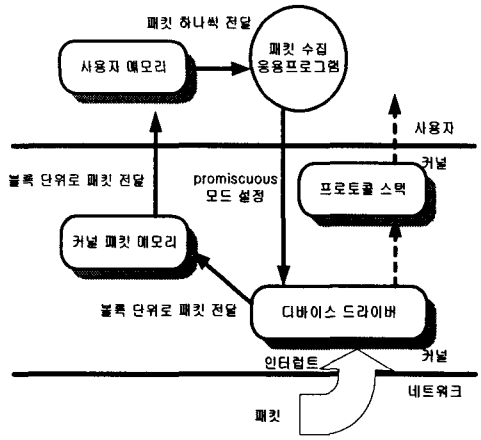


▶▶ 그림 3. tcp 패킷 분류 과정

DDoS 공격이 없는 경우 tcp 연결의 생성과 종료는 재전송의 경우를 제외하면 거의 동일한 비율로 발생할 것이다. 하지만 tcp syn flooding 공격이 발생하면 대량의 syn 플래그를 가진 tcp 패킷이 급격히 증가하므로 syn 플래그의 탐지비율이 fin 플래그의 탐지비율 보다 훨씬 많아지게 된다. 이러한 성질을 이용하여 DDoS 공격 중 tcp syn flooding 공격을 효과적으로 탐지하는 방법을 제시하고 있다. 하지만 이 방법은 tcp 연결 생성의 특성을 이용하는 방법으로 tcp syn flooding 공격의 탐지에는 매우 유용하지만 그 이외의 다른 DDoS 공격 유형에 대해서는 탐지할 수 없는 단점을 가지고 있다.

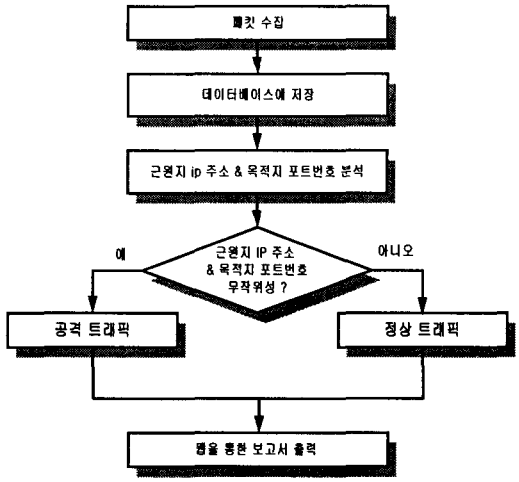
III. 패킷 분석을 통한 공격 트래픽 탐지

패킷 캡쳐를 이용한 패킷 수집 방법은 이더넷 디바이스 드라이버를 promiscuous 모드로 설정 후 패킷을 수집한다. promiscuous 모드로 설정하면 시스템이 위치한 네트워크 포인트의 모든 패킷을 수집할 수 있기 때문이다. 그림 4는 패킷 캡쳐 라이브러리를 이용한 패킷 수집 과정이다.



▶▶ 그림 4. 패킷 캡쳐를 이용한 패킷 수집

시스템에 패킷이 들어와 이더넷 디바이스에 감지가 되면 디바이스 드라이버에서 인터럽트를 건다. 그리고 디바이스 드라이버에서는 시스템에 감지된 모든 패킷을 복사해서 커널의 패킷 메모리에 저장한다. 또 이렇게 커널 패킷 메모리에 저장된 패킷들을 패킷 수집 어플리케이션이 읽을 수 있도록 다시 사용자 메모리에 복사한다. 마지막으로 사용자 메모리에 저장된 패킷을 패킷 수집 어플리케이션이 하나씩 읽어서 패킷의 헤더에서 패킷에 대한 정보를 살펴봄으로써 패킷 수집이 이루어진다.[5] 수집된 패킷의 근원지 ip 주소와 프로토콜별 포트번호로 구분하여 정상 트래픽과 공격 트래픽을 구분한다. 근원지 ip 주소의 동일성과 피해호스트에서 제공하는 응용프로그램의 서비스 포트일 경우 정상 트래픽에 의한 폭주로 판단할 수 있고 근원지 ip 주소의 무작위성의 특징과 제공되지 않는 포트로 폭주하는 트래픽은 공격 트래픽으로 판단할 수 있다. 그림 5는 공격 트래픽의 탐지 흐름도이다.



▶▶ 그림 5. 공격 트래픽의 탐지 흐름도

IV. 실험 및 결과 고찰

실험을 위해 ftp의 사용으로 인해 발생되는 트래픽 폭주와 udp flooding 공격에 의해 발생되는 패킷을 수집하고 패킷의 특징을 분석하여 정상 트래픽과 공격 트래픽을 구분하였다. 정상 트래픽은 근원지 ip 주소와 포트번호, 목적지 ip 주소와 포트번호가 일정한 특징을 가지고 있다. 즉 대상 시스템에서 서비스를 제공하는 목적지 포트번호로 트래픽이 발생한다는 것이다. tftp의 사용으로 발생되는 트래픽 폭주의 패킷을 수집하여 분석한 결과에서 알 수 있듯이 210.115.170.104 시스템에서 3248 포트를 이용하여 대상 시스템이 tftp를 서비스 해주는 udp의 69 포트로 트래픽이 폭주한 것을 알 수 있었다. 따라서 트래픽이 폭주하였지만 정상 트래픽으로 판단할 수 있었다. 그림 6은 tftp 사용으로 인해 발생된 패킷을 분석한 결과이다.

210.115.170.104:3248	210.115.170.110:69	UDP
210.115.170.104:3248	210.115.170.110:69	UDP
210.115.170.104:3248	210.115.170.110:69	UDP
210.115.170.104:3248	210.115.170.110:69	UDP
210.115.170.104:3248	210.115.170.110:69	UDP
210.115.170.104:3248	210.115.170.110:69	UDP
210.115.170.104:3248	210.115.170.110:69	UDP
210.115.170.104:3248	210.115.170.110:69	UDP
210.115.170.104:3248	210.115.170.110:69	UDP
210.115.170.104:3248	210.115.170.110:69	UDP
210.115.170.104:3248	210.115.170.110:69	UDP
210.115.170.104:3248	210.115.170.110:69	UDP
210.115.170.104:3248	210.115.170.110:69	UDP
210.115.170.104:3248	210.115.170.110:69	UDP
210.115.170.104:3248	210.115.170.110:69	UDP

▶▶ 그림 6. 정상 트래픽의 패킷 분석

트래픽 폭주 공격에 사용되는 패킷들은 공격의 근원지를 속이기 위하여 근원지 ip 주소를 스프핑하여 전송한다. 또한 대상 시스템에서 제공하지 않는 서비스 포트번호를 무작위로 생성하여 전송하는 특징을 가지고 있다. 그림 7은 udp flooding 공격의 패킷을 분석한 결과이다.

127.70.18.48:360	210.115.170.110:9640	UDP
127.57.199.96:5708	210.115.170.110:4292	UDP
127.169.30.42:4539	210.115.170.110:5461	UDP
127.109.156.123:409	210.115.170.110:9591	UDP
127.136.243.54:427	210.115.170.110:9573	UDP
127.92.250.123:4688	210.115.170.110:5312	UDP
127.99.250.50:4845	210.115.170.110:5155	UDP
127.220.224.27:4558	210.115.170.110:5442	UDP
127.229.223.35:5063	210.115.170.110:4937	UDP
127.213.40.30:4691	210.115.170.110:5309	UDP
127.246.104.109:4803	210.115.170.110:5197	UDP
127.145.103.63:4846	210.115.170.110:5154	UDP
127.91.93.3:874	210.115.170.110:9126	UDP
127.209.93.75:5607	210.115.170.110:4393	UDP

▶▶ 그림 7. udp flooding 공격의 패킷 분석

트래픽 폭주에 사용된 패킷들을 분석하면 공격 트래픽을 탐지할 수 있다. udp flooding 공격에 사용된 패킷을 수집하여 분석한 결과에서 살펴보면 127.70.18.48, ..., 127.209.93.75 등의 근원지 ip 주소와 360, ... , 5607 등의 근원지 포트번호의 무작위성과 9640, ... , 4393 등의 대상 시스템에서 제공하지 않는 서비스 포트번호를 무작위로 생성하여 공격 트래픽을 발생시킨 것을 알 수 있다. 이렇게 공격 트래픽을 탐지할 수 있었다.

V. 결론

본 논문에서는 트래픽 폭주 공격을 탐지하기 위한 패킷 분석 방법을 제안하였다. 트래픽 폭주 공격의 대응을 위해서는 트래픽 폭주 탐지되었을 경우 정상 트래픽과 공격 트래픽을 탐지하여 대응하는 것이 가장 중요하다. 실험을 통하여 트래픽 폭주를 발생시킨 패킷을 수집하고 분석하여 공격 트래픽을 정확히 탐지할 수 있음을 확인하였다. 하지만 트래픽을 수집하는 과정에서 많은 시스템 자원이 사용됨을 알 수 있었다. 차후에 적은 시스템 자원을 사용하여 트래픽 정보의 수집과 분석을 통한 트래픽 폭주 공격을 탐지할 수 있는 기술적 연구가 필요하다. 본 논문에서 제안한 패킷 분석을 통한 트래픽 폭주 공격의 탐지 기법을 침입 탐지 시스템에 적용한다면 네트워크 와 시스템 자원을 보호하여 인터넷 사용자로 하여금 정상적인 서비스를 받을 수 있을 것으로 기대된다.

▌참고문헌▌

[1] 정현철, 변대용, "트래픽 분석을 통한 서비스 거부공격 추적", 한국정보보호진흥원, 2003.

[2] 원승영, 한승완, 서동일, 김선영, 오창석, "패킷 마킹을 이용한 해킹경로 역추적 알고리즘", 한국콘텐츠학회논문지, 제3권 제1호, pp.21-30, 2003.

[3] D. Moore, G. M. Voelker, S. Savage, "Inferring Internet Denial of Service Activity," Univ. of California, 2001.

[4] H. Wang, D. Zhang, K. G. Shin, "Detecting SYN Flooding Attacks", Univ. of Michigan, 2002.

[5] 홍순화, "로트 분산 방법을 이용한 네트워크 트래픽 모니터링 및 분석", 포항공과대학교 대학원 석사학위논문, 2002.