Anti-DDoS SW 성능평가에 관한 연구

이재근* · 조인준* · 신석규**· 김선주**

*배재대학교 컴퓨터공학과 · ** 한국정보통신기술협회

Research of Anti-DDoS SW Efficiency Test

Jae-Guen Lee* · In-June Jo* · Seok- Kyoo Shin** · Sun-Joo Kim**

*Dept. of Computer Engineering Pai Chai University · **TTA

E-mail : *seoulfootballclub@pcu.ac.kr · *injune@pcu.ac.kr · **skshin@tta.or.kr · **sunjoo@tta.or.kr

요 약

최근의 인터넷 공격의 화두는 네트워크의 트랙픽을 이용한 분산 서비스 거부 (DDoS : Distributed Denial of Service) 공격이다. 정부 기관과 기업들은 DDoS 공격을 막기 위한 대응책으로 DDoS 방어 전문 장비인 Anti-DDoS SW를 도입하고 있다. 하지만 현재 Anti-DDoS의 객관적인 품질평가 기준이 없어 Anti-DDoS SW를 개발한 회사들이 제시하는 객관적이지 않은 정보에 의존하여 Anti-DDoS SW를 도입하고 있다. Anti-DDoS SW 시장규모가 커지면서 Anti-DDoS SW의 객관적인 품질평가가 요구 되고 있다.

본 논문에서는 DDoS 공격을 막기 위한 Anti-DDoS SW 제품 도입시 고려할 성능평가 요소에 대해 기술하였다.

ABSTRACT

From the recent, an big issue of the internet attack is DDoS(Distributed Denial of Service). Some government agencies and companies will buy Anti-DDoS SW for protect their their network system form DDoS attack. But We don't have any objective valuation standard of Anti-DDoS SW. So When you try to buy an Anti-DDoS SW, you can get only subjective Anti-DDoS SW information which from Anti-DDoS SW vender. Anti-DDoS SW market is getting bigger, so market needs objective valuation standard of Anti-DDoS SW for a fair evaluation.

In this paper, we describe a part of Anti-DDoS SW performance tests in valuation standard of Anti-DDoS SW.

키워드

Anti-DDoS SW, 품질평가, 성능평가, DDoS

Ⅰ. 서 론

DDoS(Distributed Denial of Service)는 분산서비스거부공격 이라 부르며, DoS(Denial of Service) 공격이 발전한 형태이다. 기존의 DoS 공격은 공격목표 호스트로 대량의 트래픽을 발생시켜서 대상 호스트의 네트워크 서비스기능을 일시적으로 또는 완전히 정지시키는 공격 유형이다. DoS 공격이 하나가 아닌 여러 개의 호스트로부터 동시다발적으로 인터넷을 공격하여 인터넷 서비스의 지연이나 마비상태에 이르게 하는 공격이 DDoS 공격이다. DoS에 대한 용어는 1999년에 등장하였으며 DoS 공격에 대한 초기공격 방식은 카네기멜론의 CERT(Computer Emergency Response Team) 권고안에 "TCP SYN Flooding and IP Spoofing Attacks" (CA-1996-21)이 1996년에 발표되었다.[1]

최근 발생한 7.7 DDoS 대란은 한국, 미국, 일본, 중국, 러시아 등의 16개국의 86개의 서버들이 사용 되었으며 감염된 8만 여대의 좀비 PC들이 백악관과 청와대, 국회, 국방부등의 정부 기관 및 기업 사이트들을 공격했다. 그 결과 정부와 기업

들 에서는 Anti-DDoS SW의 도입을 검토하고 있고 이미 도입하기로 한 곳에서는 도입 시기를 앞당기고 있다.

관련연구 에서는 2.1 DDoS 공격 분류, 2.2 봇넷(Botnet)을 이용한 DDoS 공격, 2.3 Anti-DDoS SW 네트워크 구성, 2.4 소프트웨어 품질평가 모델 ISO/IEC 9126에 대해 기술했다. Ⅲ.에서 Anti-DDoS 성능평가에 대해 기술했고, Ⅳ 결론으로 구성 했다.

Ⅱ. 관련 연구

2.1 DDoS 공격 분류

DDoS 공격에는 크게 대상 호스트를 마비시키기 위한 공격과 대상 네트워크를 마비시키기 위한 공격으로 나눌 수 있다[2][3].

호스트를 마비시키기 위한 공격은 다음과 같다.

· 7 계층(응용계층) 공격: 특정 호스트 내의 응용계층에 대한 DDoS 공격으로 정당한 사용자의 서비스를 제한하는 공격이다. 공격의 종류로는 HTTP Get Flooding 공격, Cache Control 공격, VOIP/SQL/RPC 공격 등이 있다.

· 4 계층(TCP/UDP) 공격: 특정 호스트의 모든 네트워킹 서비스 혹은 시스템 자체를 마비시키기 위해 4 계층에 대해 시도 되는 공격이다. 공격의 종류로 TCP SYN 공격, SYN-ACK 공격, RESERT Flooding 공격, UDP Flooding 공격 등이 있다.

· 3 계층(IP, ARP, ICMP) 공격 : 특정 호스트의 모든 네트워킹 서비스 혹은 시스템 자체를 마비시키기 위해 3 계층에 대해 시도 되는 공격이다. 공격의 종류로 IP Flooding 공격, ARP, RARP Spoofing 공격, ICMP Flooding 공격 등이 있다.

네트워크를 마비시키기 위한 공격은 다음과 같다[2][3].

· 중요노드 공격: 공격 대상 네트워크 내의 중요 자원에 대한 공격으로 DNS, 라우터, 병목링크 등이 대상이다. 공격의 종류로 DNS Lookup Flooding 공격, SYN Flooding 공격을 이용한 네트워크 장비의 세션관리 기능을 마비시키는 공격이 있다.

· 대역폭 소비 공격: 한정된 대역폭을 갖는 네트워크 회선 상에 막대한 공격 트래픽을 전송함으로써 네트워크를 마비시키는 공격이다. 공격의 종류로 UDP Flooding 공격, ICMP Flooding 공격이 있다.

· 네트워크 인프라 공격: 전체 인터넷 망 자체를 마비시키기 위한 공격이다. 공격의 종류로 루트 DNS 서버 공격, 대형 백본 라우터 및 라우팅 프로토콜에 대한 공격, 인증 서버에 대한 공격이 있다

2.2 봇넷(Botnet)을 이용한 DDoS 공격

악성 봇은 해커가 원격에서 조정을 통해 DDoS 공격뿐만 아니라, 악성코드 다운로드, 스팸메일 발송 등 다양한 악성행위가 가능하다. 자유자재로 통제하는 권한을 가진 봇 마스터에 의해 원격 조정되며 DDoS 공격에 수행할 수 있는 수천에서 수십만 대의 봇에 감염된 컴퓨터들이 네트워크로 연결되어 있는 형태를 봇넷이라 한다.

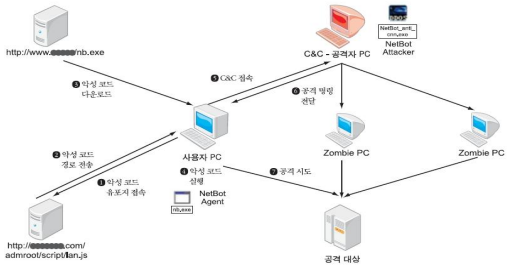

그림 1. 넷봇을 통한 DDOS 공격 개요도

2008년 부터 기존의 방식에 업그레이드 된 HTTP 봇 에 의해 DDoS 공격이 빈번하게 발생되고 있다. 기존의 악성 봇 명령/제어 서버는 주로 인터넷 채팅 프로토콜(IRC)을 이용하여 구성되었으나 최근에는 IRC 대신 HTTP 프로토콜을 이용하여 구성되고 있다. HTTP 봇의 경우 IRC 봇과 달리 윈도우즈 취약점을 직접 공격하기 보다는 유명 홈페지에 악성코드를 은닉하는 방법을 통해 사용자가 유명 홈페이지에 접속 시 자동으로 다운로드 되어 감염되도록 하여 좀비 PC를 만들어 DDoS 공격에 사용하고 있다[4].

2.3 Anti-DDoS SW 네트워크 구성

Anti-DDoS SW 네트워크 구성은 인라인 구성과 아웃오브패스 방식이 있다.

다음 그림 2.는 Anti-DDoS SW 아웃오브패스방식의 네트워크 구성도 이다.

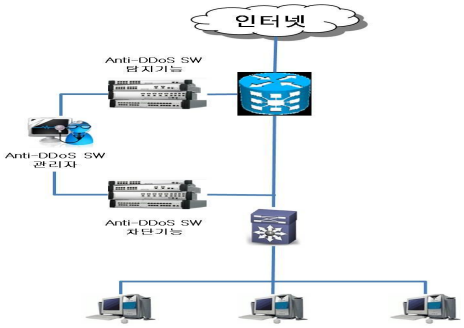

그림 2. Anti-DDoS SW 아웃오브패스 네트워크구성도

아웃오브패스 방식은 DDoS 공격을 탐지는 하되 방어 조치는 관리자가 직접 개입해 탐지된 위험에 맞게 대응하는 기법이다. 이 방식은 관리자가 직접 개입해서 탐지와 방어를 결정하기 때문에 정상적인 서비스를 방해받을 필요가 없는 장점이 있지만 반면 공격이 이미 밀려들어올 때 관리자가 방어를 지시한다 해도 이미 공격으로 피해를 받을 수 있다는 단점이 있다[5].

다음 그림 3.는 Anti-DDoS SW 인라인 네트워크 구성이다.

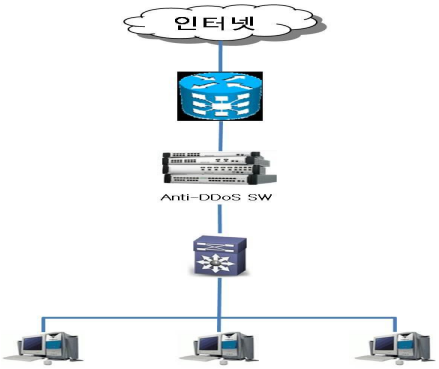

그림 3. Anti-DDoS SW 인라인 네트워크구성도

인라인 방식은 학습기법을 활용, 제로데이 즉 DDoS 트래픽이 발생하기 전 부터 공격을 탐지 자동적으로 DDoS 공격을 퇴치하는 기법이다. 이 방식은 자가 학습 기능 등으로 고객 사이트에서 공격 유형을 학습해 방어한다고 하지만 오탐이 일어날 가능성을 무시할 수 없다. 오탐으로 정상적인 서비스를 비정상으로 판단해 고객 서비스에 지연을 줄 수도 있다[5].

2.4 소프트웨어 품질평가 모델 ISO/IEC 9126

ISO 9126 국제품질표준은 소프트웨어 품질의 특성을 정의하고 품질 평가의 메트릭스 를 정의한 국제표준으로 기능성(Functionality), 신뢰성(Reliability), 사용성(Usability), 효율성(Efficiency), 유지보수성(Maintainability), 이식성(Portability)의 6가지 주특성과 각각의 주특성에 속한 부특성들이 있다[6].

· 기능성: 소프트웨어가 특정 조건에서 사용될 때, 명시된 요구와 내재된 요구를 만족하는 기능을 제공하는 소프트웨어 제품의 능력을 의미한다. 기능성은 적합성, 정확성, 상호운영성, 보안성, 준수성 등의 품질 부특성으로 세분화 된다.

· 신뢰성: 명세된 조건에서 사용될 때, 성능 수준을 유지할 수 있는 소프트웨어의 능력을 의미한다. 신뢰성은 성숙성, 오류허용성, 회복성, 준수성 등의 품질 부특성으로 세분화 된다.

· 사용성: 명시된 조건에서 사용자가 이해하고, 학습하고, 사용하며, 선호할 수 있는 소프트웨어의 능력을 의미한다. 사용성에는 이해가능성, 학습 가능성, 운영성, 선호도, 준수성 등의 품질 부특성으로 세분화 된다.

· 효율성: 명시된 조건에서 사용되는 자원의 양에 따라 요구된 성능을 제공하는 소프트웨어의 능력을 의미한다. 효율성에는 시간 효율성, 자원 효율성, 준수성 등의 품질 부특성으로 세분화 된다.

· 유지보수성: 소프트웨어가 변경되는 능력을 의미한다. 변경에는 환경과 요구사항 및 기능적 명세에 따른 소프트웨어의 수정, 개선, 또는 개작 등이 포함된다. 유지보수성에는 분석성, 변경성, 안정성, 시험가능성, 준수성 등의 품질 부특성으로 세분화 된다.

· 이식성: 한 환경에서 다른 환경으로 전이될 수 있는 소프트웨어의 능력을 의미한다. 이식성에는 적응성, 설치가능성, 대체성, 공존성, 준수성 등의 품질 부특성으로 세분화 된다.

다음 3장에서는 ISO/IEC 9126을 토대로 Anti-DDoS SW 성능평가를 위한 항목을 도출 하였다.

III. Anti-DDoS SW 성능평가

Anti-DDoS SW 의 성능평가를 위해 ISO/IEC 9126 에 속하는 6가지 주특성 중에 효율성 항목을 사용한다. ISO/IEC 9126 효율성 항목은 시간 효율성, 자원 효율성, 준수성 등의 부특성을 가진다. 시간 효율성은 규정된 조건에서 기능을 수행할 때 적절한 시간 처리 반응을 하는지에 대한 제품의 능력을 평가하는 것 이고, 자원 효율성은 규정된 조건에서 기능을 수행 할 때 적절한 자원의 양과 종류를 사용하는 소프트웨어 제품의 능력을 평가하는 것이다.

3.1 성능평가항목 도출

ISO/IEC 9126-2에 있는 품질특성에 따라서 Anti-DDoS SW의 성능평가를 위한 Anti-DDoS SW 의 품질특성 중 효율성 평가는 다음 표와 같다.

표 1 Anti-DDoS SW 효율성 평가

효율성평가	내용
시간효율성	제품 운영시 요청 이벤트에 대한 반응시간을 측정하여 평가한다.
자원효율성	제품 운영시 시스템의 자원 변화율을 측정하여 평가한다.

다음은 표2는 Anti-DDoS SW의 품질특성 중 효율성 평가 항목에서 Anti-DDoS SW 성능평가를 위한 항목을 도출 이다.

표 2 Anti-DDoS SW 성능평가항목

성능평가항목	내용
반응시간	Anti-DDoS SW가 DDoS 공격을 탐지하고 차단하는 동안 정상 패킷들이 목적지에 지연도착의 발생을 평가 하는 항목
시스템 성능	Anti-DDoS SW가 DDoS 공격에 자원을 사용하여 트래픽을 처리하는 시스템 성능에 대한 평가항목
성공율	Anti-DDoS SW가 DDoS공격을 탐지하고 차단하는 동안 정상 패킷들이 Anti-DDoS SW를 통과하여 목적지에 정상 패킷들이 100% 도착했는지에 관한 평가 항목

3.2 성능평가를 위한 테스트 베드 제안

성능평가를 위한 Anti-DDoS SW 테스트 베드 구성시 관련연구 2.3에서 언급한 네트워크 구성중 인라인 구성제품 과 아웃오브패스 구성제품을 구분하여 테스트 하여야 한다.

앞에서 도출된 성능평가 항목에 대해 시험을 위한 Anti-DDoS SW 테스트 베드를 그림 4.와 같이 제안한다.

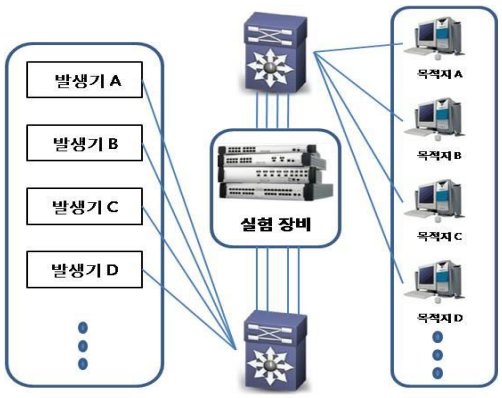

그림 4. Anti-DDoS SW 성능평가 테스트베드

발생기 A, B, C, D 는 DDoS 공격 패킷을 발생과, 정상적인 패킷을 발생 시키는 일을 한다. 발생기에서 다양한 DDoS 공격을 위한 여러 가지 DDoS 공격 툴이 사용된다. 발생기들은 실험장비에 많은 양의 트래픽을 보내기 위해 다수의 발생기 설치가 가능하다. 실험 장비는 성능 테스트를 하려고 하는 Anti-DDoS SW를 말한다. 목적지 A, B, C, D 는 DDoS 공격의 목표인 동시에 정상패킷의 도착지 이다. 이곳에서 실험결과를 위한 패킷들을 수집하는 장치가 있다.

3.3 Anti-DDoS SW성능 테스트 항목

테스베드에 시험할 Anti-DDoS SW 성능 테스트 항목은 다음과 같다.

표 3 Anti-DDoS SW 성능 테스트 항목

테스트항목	DDoS 공격	결과
7계층(응용계층) DDoS 공격에 따른 처리율, 지연, 시스템 성능	-HTTP GET Flooding공격 -Cache Control 공격 -HTTP GET Flooding + Cache Control 공격	· 처리율: 출발 패킷/도착패킷 · 지연: 패킷의 지연 도착 · 시스템성능: 장비 부하율
4계층 DDoS 공격에 따른 처리율, 지연, 시스템 성능	-TCP Flooding 공격 (SYN, ACK, Flag) -UDP Flooding 공격 -TCP + UDP Flooding -non-Spoofing 공격 과 Spoofing 공격	· 처리율: 출발 패킷/도착패킷 · 지연: 패킷의 지연 도착 · 시스템성능: 장비 부하율
3계층 DDoS 공격에 따른 처리율, 지연, 시스템 성능	-IP Flooding 공격 -ICMP Flooding 공격 -IGMP Flooding 공격 -IP+ICMP+IGMP Flooding 공격 -non-Spoofing 공격 과 Spoofing 공격	· 처리율: 출발 패킷/도착패킷 · 지연: 패킷의 지연 도착 · 시스템성능: 장비 부하율
7계층+4계층 DDoS 공격에 따른 처리율, 지연, 시스템 성능	-HTTP GET Flooding + Cache Control 공격 -TCP + UDP Flooding (non-Spoofing 공격, Spoofing 공격)	· 처리율: 출발 패킷/도착패킷 · 지연: 패킷의 지연 도착 · 시스템성능: 장비 부하율
7계층+3계층 DDoS 공격에 따른 처리율, 지연, 시스템 성능	-HTTP GET Flooding + Cache Control 공격 -IP+ICMP+IGMP Flooding 공격 (non-Spoofing 공격, Spoofing 공격)	· 처리율: 출발 패킷/도착패킷 · 지연: 패킷의 지연 도착 · 시스템성능: 장비 부하율
4계층+3계층 DDoS 공격에 따른 처리율, 지연, 시스템 성능	-TCP + UDP Flooding -IP+ICMP+IGMP Flooding 공격 -non-Spoofing 공격 과 Spoofing 공격	· 처리율: 출발 패킷/도착패킷 · 지연: 패킷의 지연 도착 · 시스템성능: 장비 부하율
7계층+4계층 +3계층 DDoS 공격에 따른 처리율, 지연, 시스템 성능	-HTTP GET Flooding + Cache Control 공격 -TCP + UDP Flooding -IP+ICMP+IGMP Flooding 공격 -non-Spoofing 공격 과 Spoofing 공격	· 처리율: 출발 패킷/도착패킷 · 지연: 패킷의 지연 도착 · 시스템성능: 장비 부하율

3.4 Anti-DDoS SW 성능 테스트 시나리오

테스트베드를 이용한 Anti-DDoS SW 성능테스트 항목별 시나리오는 다음과 같다.

표 3 에 있는 테스트 항목 순서로 테스트를 한다.

1단계) 발생기에서 정상 패킷과 테스트 항목별 DDoS 공격을 발생 시킨다.

2단계) 발생된 패킷들이 실험장비를 통과한 후 목적지에 도착한 패킷의 시간과 양을 기록하고 시스템 부하율도 기록한다.

3단계) 1시간 단위로 패킷의 양을 증가 시키고 도착지에 도착하는 패킷의 시간과 양을 기록하고 시스템 부하율도 기록한다.

4단계) 실험장비가 제공하는 대역폭 까지 트래픽을 발생 하여 테스트 한다

5단계) 기록한 값들을 가지고 반응시간, 시스템 성능, 성공률의 시간 축과 트래픽증가 축으로 해서 그래프를 만들어 성능테스트 결과 값을 만든다.

Ⅳ. 결 론

본 논문에서는 Anti-DDoS SW 성능평가에 대해 연구·분석 하였다. ISO/IEC 9126 효율성 평가 항목 토대로 Anti-DDoS SW 성능평가를 위한 성능평가 항목을 도출 하였고 성능평가를 위한 테스트 베드를 구성 하였다. 테스트 항목을 바탕으로 테스트 베드를 이용한 테스트 시나리오를 작성했다.

본 연구에서 제시한 테스트 항목과 테스트 시나리오를 바탕으로 Anti-DDoS SW를 도입 하고자하는 정부기관 및 IT업체들이 Anti-DDoS SW의 객관적인 성능평가를 할 수 있다. 객관적인 성능평가로 Anti-DDoS SW 개발 업체들은 자사 제품의 품질 향상을 위해 노력 할 것으로 예상된다.

앞으로의 과제로 본 논문에서 제시한 Anti-DDoS SW 성능평가 테스트베드를 구현하고 본 논문에서 제안한 시나리오를 바탕으로 실질적인 Anti-DDoS SW 테스트가 필요하다.

참고문헌

[1] CERT/CC Advisories, http://www.cret.org/advisories

[2] 보안게이트웨이연구팀, “분산서비스거부(DDoS)공격 대응기술 개발”, ETRI, 2009

[3] 전용희, 장종수, 오진태, “DDoS 공격 및 대응 기법 분류”, 정보보호학회지, 제19권 제3호, pp46-57, 2009.

[4] 인터넷침해사고대응지원센터, “인터넷침해사고 동향 및 분석 월보”, 2008. 8.

[5] 데이터월드, “Information Security All Guide V.4", 2009.

[6] 지식경제부기술표준원, “KS 정보기술-소프트웨어 공학-제품품질 (ISO/IEC TR 9126)", 2008.