Anti-DDoS SW BMT 평가항목 도출

신숙조* · 이재근* · 조인준* · 신석규**

*배재대학교 · **한국정보통신기술협회

BMT Derivation of Evaluation Item about Anti-DDoS SW

Suk-Jo Shin* · Jae-Guen Lee* · In-June Jo* · Seok Kyoo Shin**

*Pai Chai University · **Telecommunications Technology Association

E-mail : *{sukssj, injune}@pcu.ac.kr · **skshin@tta.or.kr

요 약

DDoS(Distribute Denial of Service) 공격은 해커가 감염시킨 개인용 컴퓨터(PC) 또는 서버 여러 대로 공격을 하게 하여 특정 시스템의 자원을 고갈시킴으로써 시스템이 더 이상 정상적인 서비스를 할 수 없도록 만드는 공격 방법이다. 최근 국내외에 발생한 DDoS 공격은 정부, 금융기관, 심지어 보안업체 시스템까지 공격을 받는 상황이다. 이러한 추세에 대응하기 위해 각 보안업체들은 DDoS 공격을 탐지하고 방어하는 제품이 개발되어 판매되고 있는 실정이다. 하지만, DDoS 제품을 서로 비교 평가 할 수 있는 기준이 마련되어 있지 않은 실정이다.

본 논문에서는 Anti-DDoS 제품들의 품질특성을 조사 분석하여 이들을 비교 평가 할 수 있는 평가 항목을 도출 하였다.

ABSTRACT

DDoS attacks make people can't using normal internet service, because DDoS attacks cause exhaustion of network bandwidth or exhaustion of computer system resources by using many personal computers or servers which already infected computer virus from hackers. Recent DDoS attacks attack government brach, financial institution, even IT security company. IT security companies make Anti-DDoS product for defense from DDoS attack. But, There is no standard for BMT of Anti-DDoS product.

In this dissertation, Anti-DDoS product quality characteristics of the survey analysis to evaluate them by comparing the assessment items were derived.

키워드

Anti-DDoS, DDoS, BMT, 평가항목

Ⅰ. 서 론

우리나라의 컴퓨터는 가전제품처럼 누구나 가지고 있고 어디든 인터넷이 연결되어져있다. 우리나라의 특성상 인터넷의 의존도가 높고 이러한 네트워크 환경에서 시스템 해킹, 악성코드, 서비스 거부 공격 등 개개인 및 주요기관을 공격 대상으로 위협받고 있다. 이러한 공격들 중에 DDoS (Distributed Denial of Service)는 네트워크 내의 수많은 시스템을 해킹한 후, 마스터 프로그램과 봇이라는 에이전트 프로그램을 설치하여 공격자가 다수의 에이전트를 이용하여 하나의 시스템을 공격하는 방식이다. 최근 대규모 사이버테러인 7.7 DDoS 공격이 진행되었는데 이 공격에 의해 감염된 8만 여대의 좀비 PC들은 일제히 국내 주요 정부기관과 금융기관, 특정 기업 사이트를 공격하여 접속 불능상태를 만들었다. DDoS 공격은 이번 7.7 대란 사태에 처음 사용된 기법은 아니다. DDoS 공격은 자기 능력을 과시하려는 수단으로 예전부터 해커들에게 이용되어 왔다. 하지만 최근 들어서 금품을 요구하는 것과 같이 뚜렷한 목적을 가지고 공격하는 성격이 뚜렷해지고 있다. 정부기관, 금융권 홈페이지, 쇼핑몰, 게임회사 홈페이지 등으로 공격하려는 대상이 중요 사이트로 많이 옮겨지고 있다. 이러한 추세로 인해 Anti-DDoS SW 제품에 대한 관심이 높아지고 있다.

현재 출시되고 있는 Anti-DDoS SW의 기본 원리는 기업 네트워크 단에 설치되어 유입되는 트래픽을 감시하며 급격하게 트래픽이 증가하거나,

DDoS로 의심되는 트래픽의 유형이 발견될 경우, 해당 트래픽을 바로 제거하는 방식이다. 처리할 수 있는 트래픽 용량이 넘어 섰을 경우 보안 제품의 처리속도와 용량을 고려해야 한다는 것과 가격이 상당히 고가라는 점이 Anti-DDoS SW가 갖는 한계라는 지적도 있다. 그럼에도 불구하고 Anti-DDoS SW의 공급이 정부기관, 금융기관을 비롯한 다양한 업체에 활발하게 이루어지고 있다. 이러한 DDoS 공격을 방어하는 제품이 국·내외에 많이 유통되고 있으나 이들을 비교평가 할 수 있는 기준이 마련되어 있지 않은 실정이다. 따라서 Anti-DDoS SW제품의 객관적인 평가모델이 필요하다. Anti-DDoS SW 품질을 측정평가하기 위해서 ISO/IEC 9126을 기반으로 평가항목을 도출하였다.

II. 관련 연구

2.1 ISO/IEC 9126

ISO/IEC 9126은 품질 특성 및 각 품질특성별로 세부 메트릭을 정의하고 있는 표준으로 소프트웨어 품질 특성과 척도에 관한 지침서로 제시되어 있다.

국제 표준인 ISO/IEC 9126은 기능성, 신뢰성, 사용성, 효율성, 유지보수성, 이식성의 6가지 품질 특성을 정의하고 있으며 각각의 품질특성은 하부에 품질 부특성 23개를 포함하고 있다.

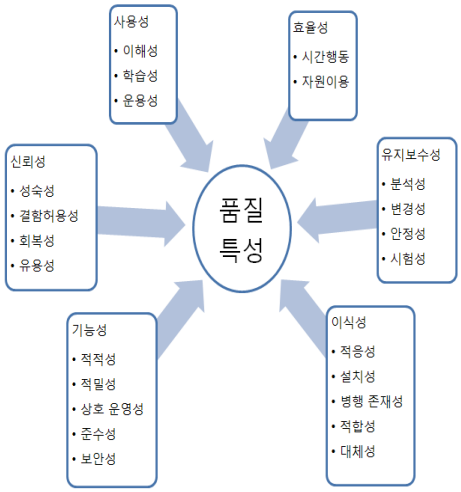

그림 1 SW 6가지 품질 특성

■ 기능성(Functionality)

소프트웨어가 특정 조건에서 사용될 때, 명시된 요구와 내재된 요구를 만족하는 기능을 만족하는 기능을 제공하는 소프트웨어 제품의 능력을 평가 한다. 제품설명서와 사용자 설명서를 기준으로 하여 제품에 대한 기능을 먼저 확인하고 기능별 평가를 할 수 있도록 테스트 케이스를 작성한다. 특히 소프트웨어 제품에 대한 기본적인 사항이 제대로 명시 되었는지 확인한다.

■ 신뢰성(Reliability)

소프트웨어가 규정된 조건에서 사용될 때 규정된 성능 수준을 유지하거나 사용자로 하여금 오류를 방지할 수 있도록 하는 소프트웨어 제품의 능력을 평가한다. 제품이 갑자기 다운되거나 결함에 의해서 제대로 결과를 수행할 수 없을 때 이것을 평가 한다.

■ 사용성(Usability)

소프트웨어가 규정된 조건에서 사용될 때, 사용자에 의해 이해되고, 학습되며 선호될 수 있게 하는 소프트웨어 제품의 능력을 평가한다. 인터페이스 측면에서 고려하여 테스트 케이스를 구성하게 되며 사용자가 잘못하여 오류를 범하였을 경우 그것에 대한 적절한 메시지가 전달되어지는지도 평가항목이 될 수 있다.

■ 효율성(Efficiency)

소프트웨어가 규정된 조건에서 사용되는 자원의 양에 따라 요구된 성능을 제공하는 소프트웨어 제품의 능력을 평가한다. 자원효율성과 시간효율성으로 나눌 수 있으며 온라인 상태에서 사용되어지면서 시간효율성에 대한 형가가 중요시 인식되어지고 있다.

■ 유지보수성(Maintainability)

소프트웨어 제품을 변경할 수 있는 능력을 평가한다. 변경에는 운영환경과 요구사항 및 기능적 사양에 따른 소프트웨어의 수정, 개선, 혹은 개작 등이 포함된다.

■ 이식성(Portability)

다양한 환경에서 운영될 수 있는 소프트웨어의 능력이다. 시스템의 구조 변경 정보 및 설치/제거 가능 여부, 타 응용시스템에 영향이 있는지의 여부, 제품의 업그레이드 후 과거 버전과의 호환 여부 등을 평가한다.

III. Anti-DDoS SW 평가 기준

Anti-DDoS에 대한 주요 기능에 대하여 ISO/IEC 9126의 6가지 평가항목을 기반으로 Anti-DDoS SW 평가 항목을 도출 하였다.

3.1 Anti-DDoS SW 기능성

■ 공격방어

- 대역폭 공격(SYN, UDP, ICMP Flooding 등)에 대한 방어 기능
- 어플리케이션 공격(FTP, Time, VoIP, Email, DNS 공격 등)에 대한 방어 기능

- 커넥션 기반 공격(HTTP Get Flooding, 파이프라인 공격 등)에 대한 방어 기능

■ 공격탐지
- 유해 트래픽 탐지 기능
- 임계치 초과 트래픽 탐지 기능
- 사용자 정의 패턴에 의한 탐지 기능
- 서비스/포트 스캐닝 탐지 기능
- 포트 사용량 분석 기능
- 트래픽 사용량 분석 기능

■ 운영관리
- 인증관리 기능
- 개인정보 검색 및 실시간 차단 기능

■ 실시간 관제
- 실시간 트래픽 상태 확인 기능
- 트래픽 수집 및 분석 기능
- 사용자 지정별 트래픽 실시간 모니터링 기능

■ 이벤트 분석
- 공격자 IP,피해자 IP 기록 기능
- 시간 및 공격횟수 기록 기능
- 기록된 데이터의 비교분석 기능
- 백업 및 리포트 기능

3.2 Anti-DDoS SW 신뢰성

■ 트래픽 과부하
- 트래픽 과부하시, 시스템이 정지/다운의 여부 확인
- 트래픽 과부하시, 트래픽의 우회 여부 확인

3.3 Anti-DDoS SW 사용성

■ 통합 기능 관리
- 실시간 모니터링 운영을 위해 사용자가 모니터링 툴의 운영 및 사용여부 확인
- 모니터링 이벤트 발생 시 사용자가 메시지 이해와 처리 가능여부 확인

■ 통계 및 보고서
- 이벤트 발생 시 나오는 통계 및 보고서에 대한 사용자의 이해 여부 확인

3.4 Anti-DDoS SW 효율성

■ 시간 효율
- 이벤트 발생 시 처리시간
- 트래픽 실시간 탐지/분석
- 트래픽 발생시 DDoS공격 유무 확인 시간

■ 자원 효율
- 트래픽 과부하시 CPU/메모리 사용량 분석

3.5 Anti-DDoS SW 유지보수성

■ 시스템 분석 및 변경
- 시스템 운영 중 발생하는 이벤트에 관한 메뉴얼 여부 확인
- 시스템 환경 설정 변경 제공 여부 확인

3.6 Anti-DDoS SW 이식성

■ 시스템 설치 및 연동성
- 타 네트워크 단에서의 기본 설정의 원활한 서비스 제공 여부 확인
- 다양한 네트워크 환경에서의 설치/제거 여부 확인
- 타 보안장비(방화벽, IPS, UTM 등)의 호환성 여부 확인

위에서 열거한 Anti-DDoS SW 6가지 평가항목을 기술하면 [표 1] 과 같다

표 1. Anti-DDoS 평가 항목

품질 특성	평가 항목
기능성	- 대역폭, 어플리케이션, 네트워크 기반에 대한 공격 방어 - 유해 및 임계치 초과 트래픽 탐지 - 사용자 정의 패턴에 의한 탐지 - 포트 및 트래픽 사용량 분석 - 개인 정보 인증 관리 - 실시간 트래픽, 검색의 실시간 차단 - 공격자, 피해자 IP 기록 확인 - 이벤트 발생 시간 및 공격횟수 확인 - 데이터의 비교분석 및 백업, 리포트
신뢰성	- 트래픽 과부하시 시스템 정지/다운 여부를 확인 - 시스템이 정지/다운되지 않도록 트래픽의 우회 여부 확인
사용성	- 실시간 모니터링 툴에 대한 사용자의 운영 이해와 사용 가능 여부 확인 - 이벤트 메시지와 처리 철차를 사용자가 이해 가능여부
효율성	- 트래픽 발생 실시간 탐지/분석 및 트래픽 이벤트 처리 시간의 적절성 확인 - 트래픽 공격 시 DDoS 공격 유무 확인 시간의 적절성 확인 - 트래픽 발생시 CPU/메모리 자원의 사용률의 적절성 확인
유지 보수성	- 시스템 운영 중의 발생하는 이벤트에 관한 처리 메뉴얼의 여부 - 시스템 환경을 사용자 정의에 의한 설정 변경 여부
이식성	- 기본 시스템설정이 타 네트워크에서의 원활한 서비스 제공 여부 - 다양한 네트워크 환경에서의 설치/제거 여부 - 다른 보안장비와의 연동성과 호환성 여부

Ⅳ. 결 론

본 논문에서는 ISO/IEC 9126을 기반으로 Anti-DDoS SW 평가항목을 도출하였다. Anti-DDoS SW를 도입 시 각 평가항목을 참고하여 제품을 선택하고, 보안업체는 본 논문에서 기술된 평가항목을 참고하여 개발해야 할 것이다.

현재에도 다양한 유형의 DDoS 공격 패턴이 출현하고, 그에 따른 Anti-DDoS SW에 필요한 공격 탐지 기능 및 추가 기능의 지속적인 개선이 필요하다. 그 중에서 제품의 성능에 대한 고려가 가장 중요한 잣대로 작용한다. 따라서, 향후 효율적인 제품의 성능 평가방안에 대한 연구가 필요하다.

참고문헌

[1] KISA, "DDoS 현황 및 대응“, 2008. 10
[2] 김선주 외 2, “통합보안관리시스템에 대한 평가항목 도출”, 한국정보처리학회 2009 춘계학술발표대회 논문집, 2009. 4
[3] ISO/IEC 9126: Software Engineering-Software Product Quality