DDoS 공격에 대한 효과적인 보안 관제 방안

정일권* · 김점구** · 김귀남* · 하옥현***

요 약

DDoS 공격은 외부의 공격자가 일반 사용자들의 PC를 감염시킨 후 감염된 PC에서 특정 웹 사이트나 서버에 대량의 트래픽을 전송하여 리소스를 고갈시키거나 네트워크 대역폭을 점유함으로써 서비스를 마비시키는 공격으로, 완벽하게 막는 것이 대단히 어렵다. IDS(Intrusion Detection System : 침입 탐지 시스템), IPS(Intrusion Prevention System : 침입 방지 시스템), ITS(Intrusion Tolerance System), FW(Firewall) 또는 DDoS 전용 보안 장비 등을 이용하여 DDoS 공격을 막아내거나, 감내하려고 한다. 여러 종류의 보안 장비 비용 문제가 발생하기도 하고, 각 시스템 간의 연계성을 고려하지 않은 설치로 제 기능을 발휘하지 못하기도 한다. 본 논문에서는 DDoS 공격에 대한 보안 장비의 효과적인 연계와 대응 방법론을 제시한다. 설계된 방법론을 적용할 경우 기존의 네트워크 구조상에서보다 DDoS 공격에 대한 차단 및 감내 효율이 실험을 통해 입증되었다. 따라서 차별화된 DDoS 공격을 대응 및 감내하는 관제 방안을 본 연구를 통해 제시하고자 한다.

Research on Effective Security Control Measures Against DDoS Attacks

Il Kwon Jung* · Jeom Gu Kim** · Kiu Nam Kim* · Ok Hyun Ha***

ABSTRACT

It is very difficult to completely block the DDoS attack, which paralyzes services by depleting resources or occupying the network bandwidth by transmitting a vast amount of traffic to the specific website or server from normal users' PCs that have been already infected by an outside attacker. In order to defense or endure the DDoS attack, we usually use various solutions such as IDS (Intrusion Detection System), IPS (Intrusion Prevention System), ITS (Intrusion Tolerance System), FW (Firewall), and the dedicated security equipment against DDoS attack. However, diverse types of security appliances cause the cost problem, besides, the full function of the equipments are not performed well owing to the unproper setting without considering connectivity among systems. In this paer, we present the effective connectivity of security equipments and countermeasure methodology against DDoS attack. In practice, it is approved by experimentation that this designed methdology is better than existing network structure in the efficiency of block and endurance. Therefore, we would like to propose the effective security control measures responding and enduring against discriminated DDoS attacks through this research.

Key words : DDoS(Distribute Denial of Service), Managed Security Service

접수일 : 2009년 10월 10일; 채택일 : 2009년 12월 11일

* 경기대학교 산업보안학과
** 남서울대학교 컴퓨터공학과
*** 교신저자, 호남대학교 경찰법행정학부

1. 서 론

최근 정보통신 기술의 빠른 발전으로 인터넷 환경 또한 크게 변화되었다. 이러한 인터넷 환경의 발전은 생활을 보다 효율적이고 편리하게 바꾸었다. 그러나 인터넷의 확장으로 인하여 보안적 측면에서 문제가 대두되기 시작하였으며, 외부의 침입자가 내부의 정보 시스템을 불법침입, 정보의 유출, 변경, 훼손 및 서비스 거부 등 보안사고가 끊이지 않고 발생하고 있다. 최근에는 일부 기업 등에서 웹 사이트나 서버에 네트워크 장애를 발생시키는 DDoS(서비스 거부) 공격이 발생하여 경제적으로 막대한 피해를 입히는 사태가 빈번히 발생하고 있다.

DDoS 공격은 공격자가 일반 사용자들의 PC에 악성 코드를 심어 감염시킨 후 감염된 PC를 이용하여 특정 웹 사이트나 서버에 대량의 트래픽을 일반적으로 업무에서 침입 탐지 시스템(IDS : Intrusion Detection System), 침입 방지 시스템(IPS : Intrusion Prevention System), 침입 감내 시스템(ITS : Intrusion Tolerance System), 방화벽(FW : Firewall) 또는 DDoS 전용 보안 장비 등을 이용하여 DDoS 공격을 막아내거나, 감내하려고 하지만, 여러 가지 보안 장비를 모두 구입하여 사용하기에는 비용적인 문제가 발생하거나, 각 보안 장비 간의 연계성을 고려하지 않은 설치로 제 기능을 발휘하지 못하기도 한다. 이상과 같은 내용을 고려해볼 때, 기업 및 단체 등에서 현실적으로 보유한 보안 시스템만으로 DDoS 공격을 효율적이고 빠른 대응 및 감내가 가능한 관제 방안을 연구해 보려고 한다.

2. 관련연구

DDoS 공격 형태는 초당 패킷 수(PPS; Packets per Second)를 증가시켜 시스템의 자원을 소비하는 공격, ICMP나 UDP를 이용하여, 네트워크 대역폭을 차지하여 데이터 전송을 막는 공격, 웹 서버의 서비스 지연 공격이 있다 최근 2009년 7월 7일에 발생한 DDoS 공격을 보면, 네트워크 기반 공격인 UDP Flooding 공격, ICMP Flooding 공격과 애플리케이션 기반 공격인 HTTP Get Flooding 공격과 CC 공격(Cache-Control Attack), 복합하여 사용하는 형태를 보이고 있다[17].

DDoS 공격에 대하여 탐지하는 기법도 여러 가지가 연구 되고 있다. 통계적 탐지 기법의 경우 [5]에서 통계적 데이터를 기반으로 DDoS 공격을 탐지 하였고, [6]에서는 데이터마이닝 기법을 이용하여 DDoS 공격을 탐지하였다. 그밖에도 [7]에서 사용한 SNMP-MIB를 이용하여 DDoS 공격을 탐지하였다. 그러나 이러한 탐지 방법들은 전체적인 탐지에 고루 쓰이지 않고, 출발지 주소, 도착지 주소 또는 포트 번호 등과 같은 특정 요소에 대한 탐지만 되거나, 대용량의 학습 데이터가 필요하다는 점과 새로운 유형에 대한 탐지가 힘들다는 점 그리고 실시간으로 유입되는 패킷들에 대한 처리 능력이 다소 떨어지는 문제점이 있다. 그러므로 최근의 연구에서는 여러 가지 탐지 기법들을 혼합하여 장점을 취하는 연구 방법이 제안되고 있다.

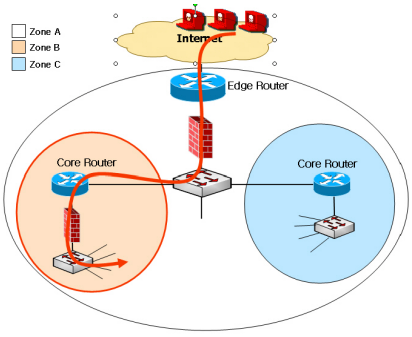
3. DDoS 공격에 대한 관제 방안

3.1 UDP/ICMP Flood 공격 대응

UDP Flood, ICMP Flood 공격은 정상적인 트래픽(normal traffic)과 비 정상적인 트래픽(anomaly traffic) 간의 차이를 분석하고 적절한 대응을 하는 것이 DoS를 방어하는 주요점이 된다.

일반적으로 UDP Flood, ICMP Flood 공격을 수행할 때 단일 Zombie PC에서 발생시키는 패킷은 그 크기가 다양하며 전송 간격 또한 다양화 하게 된다. 하지만 Firewall로 모든 패킷이 몰리게 되어

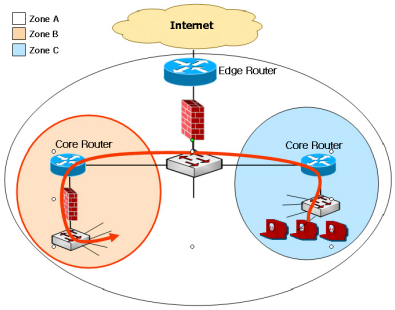
단일 시간(보통 초 단위)에 대량의 패킷이 몰릴 수 밖에 없다. 따라서 방어 및 감내를 위해 Firewall의 Threshold 설정 기능을 이용하였다. 보호하고자 하는 대상이 Zone B에 존재한다고 할 때, DDoS 공격은 크게 1) Internet 을 통한 외부 유입과 2) 내부 유입으로 나눠 생각할 수 있다. Internet을 포함한 망 외부에서 DDoS공격이 발생할 경우 (그림 1)과 같이 생각해 볼 수 있다.



(그림 1) 외부에서 DDoS 발생시

이와 같은 공격이 진행 될 경우 트래픽에 가장 큰 영향을 받는 부분은 Edge Router와 인접한 Firewall이다. 물론 공격자로부터 Edge Router를 통해 victim으로 가는 모든 네트워크의 자원이 소모되므로 DoS 상태에 빠지게 된다.

이를 방어하기 위해서는 Core Router 쪽의 Firewall이 아닌 Edge Router쪽의 Firewall에서 Threshold 설정을 해주어야 한다. 그 이유는 victim과 가까이에 있는 firewall에서 설정 해주었다 하더라도 Edge Router에서부터 bandwidth 소모가 일어나므로 결과적으로는 DDoS 상태를 빠져나올 수 없기 때문이다. 물론 가장자리(perimeter)쪽의 장비 가용성이 뛰어날 경우에는 문제를 발생시키는 Core Router쪽에서 방어를 해도 상관은 없다. 대용량의 bandwidth를 소모시키는 DDoS가 발생할 경우 Edge Router쪽에 있는 Firewall에서의 방어가 가장 효과적일 것이다. (그림 2)은 Zone B가 아닌 내부의 다른 Zone에서 DDoS 공격이 시작되는 모습을 보여주고 있다.



(그림 2) 내부에서 DDoS 발생시

이러한 형태의 공격은 기본적으로 Threshold 설정을 어디에 할 것인가와 부가적으로 Router에서의 Ingress/Egress Filter를 어떻게 할 것인가와 관련이 있다. 먼저, victim의 서비스를 정상화 시키기 위해 Zone A에 위치한 방화벽에서 적절한 Threshold 설정을 해야 한다. 다음, NMS이나 IDS/IPS를 이용하여 트래픽 분석을 실시한 후 DoS의 진원지를 파악해야 한다. 위치가 파악되면 DDoS의 진원지와 가장 근접한 Router에서의 Filter 설정과 Firewall 설정하여 다른 Zone으로 비정상적인 UDP packet이 흐르지 못하도록 해야 한다. 마지막으로, 진원지 Zone에 위치한 Host를 조사하여 서비스 거부를 발생시키는 악성 프로그램을 찾아서 제거한다.

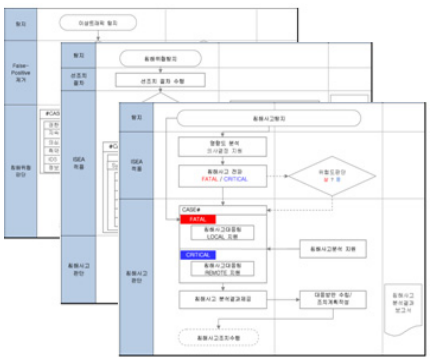
3.2 CC 공격 대응

CC 공격(Cache-Control Attack)은 HTTP User Agent 에 불필요한 값을 추가하여, 웹 서버의 오동작을 일으킨다. 공격은 수백에서 수천 개의 Zombie PC가 1분에 300개에서 400개의 Syn 패킷을 보내며, 일정 시간을 공격하다가 쉬고 다시 공격하는 양상을 띈다. 이때 보안장비를 통하여 제때 방어하지 않는다면, 짧은 시간 안에 503 error → time-wait → session full → DOS 순서로 상태가 변하게

된다. 이를 방어하기 위해서는 필수적으로 HTTP Inspection이 가능해야 하며, IDS/IPS의 signature pattern에 Cache-Control : no-store, must-revalidate를 추가하여 준다.

3.2 의사결정 프로세스

DDoS 공격 유형 별로 네트워크 정보보호 스트럭처 간의 상호 보완적인 연계와 (그림 3)과 같은 의사결정 프로세스를 통하여, DDoS 공격을 효과적으로 차단 및 감내한다.



(그림 3) 의사결정 프로세스

초기 이상징후 탐지 후 최대 30분 안에 관련 내용 분석한다. 침해 위협은 위협을 판단하는 프로세스에 따라 침해 위협과 이상트래픽(Warning)로 구분한다. 침해 사고는 사고를 판단하는 프로세스에 따라 공격 성공(FATAL/CRITICAL)과 공격실패(MINOR)로 구분한다. 침해 사고의 내용 분석 결과 심각도가 1(FATAL)과 2(CRITICAL)의 경우 원격 및 로컬에서 수행하며, 심각도 1일 경우 로컬에서 대응한다. 심각한 수준의 침해사고 및 해킹사고가 발생하여 침해사고 피해 시스템 분석이 필요한 경우 침해사고 분석 절차에 따라 침해사고 분석 및 복구 업무를 수행한다. 침해사고 분석은 준비 단계에서 철수 단계의 총 7단계로 나뉜다. 준비 단계에서는 침해사고 분석에 앞서 피해 시스템의 데이터 백업을 수행하고, 침해사고 대응에 필요한 분석/치료/대응 도구 및 원상 복구를 위한 도구 준비 및 설치한다. 분석 단계에서는 침해 시스템의 정보 수집, 시스템 프로그램의 변조 여부 점검, 중요 파일들에 대한 최종 접근 로그 확인, 시스템과 네트워크 설정 점검, 피해 시스템이 존재하는 동일 네트워크의 다른 시스템 존재 여부 점검한다. 추적 단계에서는 공격자와 공격지를 확인한 경우 역추적하여 공격지 IP, 호스트명, 시스템, 공격로그 등 수집된 공격 흔적을 통해 대응 조치하고, 공격지 확인이 불가능한 경우나 DDoS 공격 등의 자동화된 공격도구에 의한 침해사고의 경우 관련 취약점 보안 강화 조치 적용을 위해 공격 분석을 통한 네트워크 및 주변 시스템을 조사 및 분석한다. 피해 시스템의 주변에 추가적인 피해가 예상되거나 위협이 될만한 시스템 및 네트워크에 대하여 필요한 경우 추가적인 분석을 진행하고나 분석 종료한다. 치료 및 방역 단계에서는 백도어, 루트킷 등이 설치된 위치를 찾아내어 제거하거나 심각한 경우 파일시스템을 포맷하고 피해 시스템을 네트워크에서 분리하여, 운영체제, 응용 프로그램 등을 설치하여 정상 운영 될 수 있도록 한다. 복구 단계에서는 부팅 및 시스템 파일을 복구하고, 최신 어플리케이션 설치 및 취약점 패치를 수행한다. 보고 단계에서는 피해시스템을 분석하여 원인, 해결 방법, 복구 방법, 추적 결과 등을 기술한 결과보고서를 작성한다. 마지막으로 철수 단계에서는 침해사고 분석 결과 더 이상의 대응 지원 작업이 없는 경우 결과를 통지한 후 종결한다.

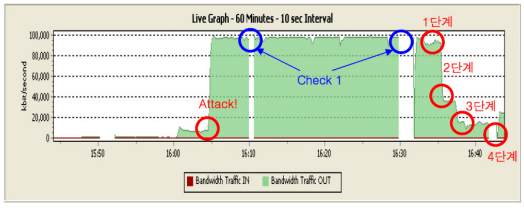
4. 시험 및 검증

제안한 보안 관제 방안의 효과를 측정하기 위하여 외부의 Zombie PC 에서 DDoS 트래픽을 발생시켰다. UDP/ICMP Flooding DDoS 공격 환경을 구성하기 위해 5대의 샘플 호스트와 rBot으로 잘

알려져 있는 IRC Bot을 이용하였다. victim agent의 무작위로 선택 된 포트를 향해 패킷 당 4096 Bytes씩 100000개를 10ms 단위로 전송하였으며, Threshold에 따른 트래픽 변화를 쉽게 확인하기 위해 아래와 같이 단계적으로 차단 Threshold를 조정하여 테스트 하였다.

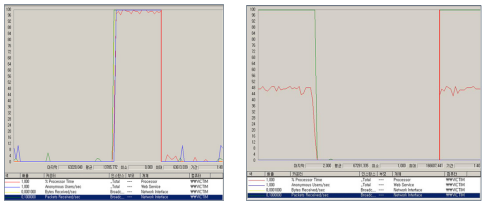
- 1단계 : 200 pps
- 2단계 : 100 pps
- 3단계 : 50 pps
- 4단계 : 20 pps

(그림 4)는 Threshold 차단을 통하여 트래픽이 감소되는 것을 나타낸다.



(그림 4) Threshold에 따른 트래픽 변화

CC-Attack 공격은 DosHTTP을 이용하여 테스트 하였다. (그림 5)에서와 같이 victim agent 의 자원 사용이 가능해지는 것을 알 수 있다.



(그림 5) CC 공격 전.후 자원 변화

(그림 6)은 DDoS 공격시 유입 트래픽 및 서버 자원 상태 및 웹 서비스 상태를 나타낸 것이다. 그림에서와 같이 제안한 관제 대응 및 프로세스를 통하여 보다 효과적으로 DDoS를 감내하는 것을 알 수 있다.

상세 항목	측정 결과												
	공격시						방어후						
	유입 트래픽(MRTG)		서버 리소스 상태(%)				유입 트래픽(MRTG)		서버 리소스 상태(%)				웹서비스 상태
	BPS	PPS	BPS	PPS	CPU	IIS	BPS	PPS	BPS	PPS	CPU	IIS	목표서버	비 목표서버
ICMP Flood	637	59000	100	100	50	1	0.008	3	4	2	1	1	정상	정상
UDP Flood	591	59000	100	100	50	20	0.008	4	2	4	1	20	정상	정상
CC Attack	73	110000	100	100	80	24	0.016	6	2	4	1	20	정상	정상

(그림 6) DDoS 공격시 변화 비교

5. 결 론

DDoS 공격은 공격 발생 수 분 안에 네트워크 인프라를 사용 불능으로 만들 정도로 강한 파괴력을 보이고 있기에 무엇보다 사고 발생 즉시 이상징후를 발견할 수 있는 환경을 조성하는 것이 중요하다. 본 논문에서는 네트워크 정보보호인프라스트럭처와 합리적인 의사결정 프로세스를 통하여 DDoS 공격 별 이상징후 조기 탐지 및 대응에 대한 문제점을 해결하였다. 향후 다량의 사례연구가 필요하며, 보다 많은 네트워크 환경 별 대응 프로세스 연구가 요구된다.

참 고 문 헌

[1] 국윤주, 패킷 연관성 기반 효율적인 DDoS 공격 탐지 모델, 경기대, 2008

[2] 김수학, 정책 기반 DDoS 공격탐지 및 대응 방안에 관한 연구, 한국외대석사논문, 2005.

[3] 구자진, 비정상 행위 탐지를 이용한 네트워크서비스거부 공격 대응 기술 연구, 동국대석사논문, 2002.

[4] 정휘석, 트래픽 분석을 통한 DDoS 공격 탐지 및 방어 방법에 관한 연구, 아주대석사논문, 2003.

[5] Laura Feinstein, Dan Schnackenberg, Ravindra Balupari, Darrell Kindred, “Statistical

Approaches to DDos Attack Defection and Response", Proceedings of the DARPA Information Survivability Conference and Exposition DISCEX'03, 2003

[6] 박정민, 나현정, 황경애, 채기준, "광역망에서의 DDOS 탐지 메커니즘에 관한 연구", 이화여자대학교, 2003.

[7] J. Li and C. Manikopoulos, "Early statistical anomaly intrusion detetion of Dos Attacks using MIB traffic parameters", Information Assurance Workshop, IEEE, pp. 53-59, 2003.

[8] Michael Glenn, "A Summary of DoS/DDoS Prevention, Monitoring and Mitigation Techniques in a Service Provider Environment", 2003.

[9] Cisco, "Worm Mitigation Technical Details", 2004.

[10] J. Postel, "USER DATAGRAM PROTOCOL", 1980.

[11] Juniper Networks, "FIPS 140-2 Security Policy", 2006.

[12] Milutinovic, Milic, Savic, "Denial of Service Attacks : Methods, Tools, and Defenses"

[13] Konstantinos, Brian, Hyoseon Kim, "The Detection and Defense of DDoS Attack".

[14] Cisco, 2004, "Defeating DDoS Attacks"

[15] Ross Oliver, "Countering SYN Flooding Denial of Service (DOS) Attack".

[16] J. Postel, "INTERNET CONTROL MESSAGE PROTOCOL", 1981.

[17] SK Infosec, MSS 사업본부/침해대응센터. "7-7 DDoS 공격 경과 및 대응방안".

정 일 권

2008년 남서울대학교 컴퓨터학과(공학사)
2008년 경기대학교 정보보호학과 석사과정

김 점 구

광운대학교 전자계산학과(이학사)
광운대학교 전자계산학과(이학석사)
한남대학교 컴퓨터공학과(공학박사)
(주)제성프로젝트 연구원
(주)시사컴퓨토피아 인터넷사업본부장
현재 남서울대학교 컴퓨터학과 교수

김 귀 남

미국 캔자스대학교(공학사)
미국 콜로라도주립대학(공학석사)
미국 콜로라도주립대학(공학박사)
현재 경기대산업기술보호특화센터 센터장
현재 경기대학교 정보보호학과 교수

하 옥 현

1978년 성균관대학교 정치외교학과(정치학사)
1980년 서울대학교 행정대학원(행정학석사)
1998년 프랑스 사회과학대학원(EHESS) 박사과정(DEA 취득)
2005년 고려대학교 정보보호대학원(공학박사)
2008년~현재 호남대학교 경찰법행정학부 교수