이중 필터링을 이용한 분산서비스 거부 방어 시스템 방법

최지훈*, 전문석*
*숭실대학교 일반대학원 컴퓨터학과
e-mail : czih@nate.com, mjun@ssu.ac.kr

A DDoS Protection System Using Dual Filtering Method

Ji-hoon Choi*, Moon-seog Jun*
*Dept of Computer, Soong-Sil University
e-mail : czih@nate.com, mjun@ssu.ac.kr

요 약

DDoS(distributed denial of service)공격은 1990년 중반에 처음 나타나기 시작하여 1,2세대 네트워크 자체에 대한 트래픽 폭주형태의 공격에서부터 3세대 봇넷을 이용하여 특정 서버와 특정서비스를 마비시키기 위한 공격을 거쳐 4세대의 분산 형식의 C&C를 이용하는 공격의 유형으로 발전 하고 있다. DDoS공격은 점점 지능화 되고 있으며 기존의 IDS(Intrusion Detection System) 시스템을 이용한 탐지방법으로 공격을 탐지하기에는 어려움이 존재한다.

본 논문은 IDS시스템을 보다 더 지능화시키기 위한 논문으로 IDS는 내부시스템으로부터 쿼리를 넘겨받아 업데이트를 수행하고 업데이트를 수행함과 동시에 라우터에게 C&C서버로부터 나오는 패킷을 차단하도록 알려 준다. 즉, IDS에서 일어나는 False Negative문제를 줄여줌으로써 DDoS 공격에 대하여 Zombie시스템을 생성하지 못하도록 하고자 하는데 그 목적이 있으며 점점 지능화되어 가고 있는 DDoS공격에 대하여 차단을 하고자 하는 방향성을 제시하고 있다.

1. 서론

최근 인터넷의 급속한 확산과 정보통신 기술의 발달로 인하여 모든 환경에서 인터넷으로 연결되어 사용하고 있으며, 이러한 상황에서 네트웍이나 서버로의 접근을 불가능 하게 하는 문제는 불편함을 벗어나 엄청난 경제적 손실을 가져오고 있다. 이러한 문제를 해결하기 위하여 가용성을 보장하는 기술력이 발전되고 있지만 사용자들의 최고 100Mbps를 제공하는 광랜을 많이 사용하고 있는 사용자 수가 늘어남에 따라 ZombiePC에서 나오는 DDoS공격은 수 Gbps의 트래픽을 유발시킬 수 있는 현실이 되어 버렸고 가용성을 보장하는 서비스를 무력화시킬 정도의 엄청난 네트웍 트래픽을 발생시키고 있다.

DDoS(Distributed Denial of Service)공격은 1990년 중반에 처음 나타나기 시작하여 1,2세대 네트워크자체에 대한 트래픽 폭주형태의 공격에서부터 3세대 봇넷을 이용하여 특정 서버와 특정서비스를 마비시키기 위한 공격을 거쳐 4세대의 분산 형식의 C&C를 이용하는 유형으로 발전 하고 있다[4].

DDoS시스템의 구성은 Attacker, Agent, Zombie, Victim으로 나뉘며 독자적인 프로토콜기반에서부터 일반적인 프로토콜을 기반으로 하여 다양한 프로토콜이 사용되고 있다. DDoS 시스템에서의 공격방식은 다수의 ZombiePC로부터 나가는 대량의 트래픽이 하나의 Victim에게 집중됨으로 Victim의 시스템 자원을 고갈시켜 정상적인 서비스나 의도된 용도로 사용하지 못하도록 한다.

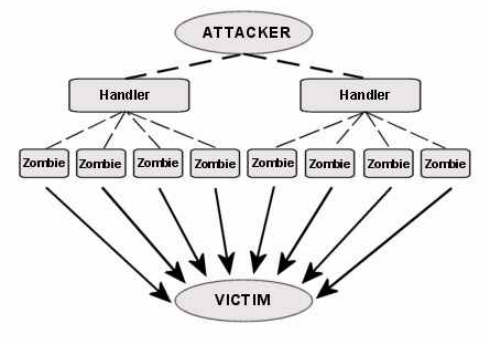
DDoS공격이 실제적으로 일어나기 전 Victim의 대상이 될 PC들은 C&C서버와 많은 메시지를 주고받는 행동을 수행하기 때문에 Victim이 될 PC에서 나오는 메시지를 내부에 구성된 모니터링 시스템을 이용하여 탐지하는 방식을 제안한다.

본 논문은 Zombie의 생성을 방지하여 실제적인 공격이 이루어지기 전에 차단함에 있으며, 완벽한 실시간을 지원하기에는 무리가 있음을 명시한다. 논문의 구성은 다음과 같다. 2장에서 관련연구로는 DDoS공격과 공격유형, 기존의 대응방법에 대하여 설명하고, 3장에서는 제안하는 DDoS방어 시스템에 대해서 설명하며, 마지막 4장에서 결론을 맺는다.

2. 관련 연구

2.1 분산 서비스 거부공격 (DDoS)

분산 서비스 거부공격은 시스템을 악의적으로 공격해 해당 시스템의 자원을 부족하게 하여 원래 의도된 용도로 사용하지 못하게 하는 공격이다. 특정 서버에게 수많은 접속 시도를 만들어 다른 이용자가 정상적으로 서비스 이용을 하지 못하게 하거나, 서버의 TCP 연결을 바닥내는 등의 공격이 이 범위에 포함된다. 대표적인 분산 서비스 거부공격 다이어그램은 [그림 1]과 같다[5].



[그림 1] DDoS 공격 다이어그램

공격자는 최초에 특정 웹사이트나 혹은 파일에 악성프로그램을 숨기거나 스팸메일 등 여러가지 방법을 거쳐 다수의 ZombiePC를 확보한 상태에서 Handler에게 공격명령을 내려서 공격을 수행하는 방식이다.

2.2 공격 유형

2.2.1 Flooding 공격

일반적으로 플러딩 공격은 정상 패킷과 동일한 패킷을 무작위로 전송하여 타깃시스템의 CPU, 메모리 등을 고갈시키고 네트웍의 병목을 발생시켜 정상적인 서비스를 방해하는 형태의 공격이다[2].

2.2.2 커넥션 기반 공격

케넥션 기반 공격은 기본적으로 지정되어 있는 연결설정 보다 초과 되는 연결을 맺게 함으로써, 정상적인 연결을 방해하는 형태의 공격을 말하는데 즉, TCP커넥션 형태의 공격처럼 TCP 연결 가능 수치를 초과하여 서버의 정상적인 연결 시도를 방해하는 공격이다[3].

2.2.3 어플리케이션 기반 공격

어플리케이션 기반 공격은 특정 어플리케이션에 대하여 해당되는 공격이다. 어플리케이션 기반 공격의 종류는 FTP, DNS, SQL 공격 등 다양한 형태의 어플리케이션 공격이 존재하며 대표적으로 Cache Contorl 공격을 예로 들자면 메모리에 있는 데이터를 이용하지 않는 방식이다. 이런 방식으로 DB에게 쿼리를 보냄으로써 요청 때 마다 웹서버는 해당 데이터를 집적 읽게 되도록 하여 CPU에 대하여 부하를 일으켜 시스템을 원활하게 사용하지 못하도록 하는 방법이다[6].

2.3 기존의 DDOS 대응 방법

2.3.1 백본 네트워크 레벨 대응

다수의 Zombie에서 공격 트래픽이 생성되어 공격 대상 시스템으로 전송되는 유형을 가지며 Zombie는 전 세계에 널리 분포되어 있기 때문에, 공격 대상시스템이 속한 국가의 백본을 거쳐 전달될 가능성이 높으므로 백본 네트워크를 모니터링하고 공격의 징후를 탐지 한다.

2.3.2 Edge 네트워크 레벨 대응

Edge 네트워크는 공격 대상 시스템으로 전달되는 모든 공격 트래픽이 통합되는 곳이므로 트래픽의 변화를 측정하여 공격 트래픽이 서버에 전달되기 이전에 공격 트래픽을 탐지하고 차단하는 곳으로 거의 모든 DDoS 공격 대응 시스템이 이 위치에서 설치되고 운영되고 있다.

2.3.3 공격 대상 서버 레벨 대응

공격 대상 서버는 우선적으로 사용자에게 서비스를 제공하여야 하기 때문에 공격 트래픽을 높은 성능으로 분석하기에는 무리가 있다. 즉, 고도의 DDoS 공격탐지 및 차단 기법을 적용하는 것이 아니라 서버에 특화된 최소한의 공격 차단 기법만을 적용하여 탐지 한다. 즉, CPU점유율 및 다양한 정보 등을 이용하여 공격 여부를 판단 한다.

2.3.4 통합 분석 레벨 대응

공격 발생 시 전역 네트워크상에서 발생하는 다양한 보안 이벤트들을 수집하여 통합 분석하고 그에 대한 분석결과를 공격 탐지 및 차단에 활용 한다. 공격에 대해 효과적으로 대응하기 위해서는 공격 관련 정보들을 수집하고 이를 자동화된 방법으로 통합 분석하여 신속히 공격을 탐지하고 그에 대한 대응 방안을 모색하며, 기존에 설치되어 있는 다양한 보안 장비들에게 현재의 공격상황에 대한 정보를 전달할 수 있어야한다[1][5].

3. 제안 시스템

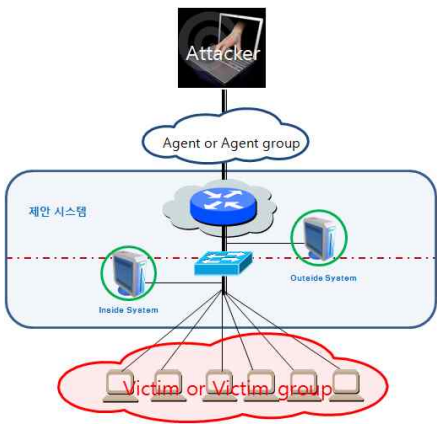
3.1 제안하는 DDoS 방어 시스템 방법

제안 시스템은 DDoS공격 이전의 메시지 흐름을 이용하여 IDS에서 일어나는 False Negative문제에 대하여 초점을 두고 있다. DDoS공격 역시 서버와 클라이언트 기반의 시스템으로 구성되므로 서버와 클라이언트 사이에는 요청과 응답이 꼭 이루어져야 한다.

제안 하는 시스템은 Victim에서 나가는 메시지에 대하여 Inside System에서 모니터링을 수행하고 IDS가 탐지 못한 패턴을 적용시켜 차후 동일한 공격 패턴이 들어 올 경우, 차단하여 False Negative를 점점 줄여나가는 방법이다.

3.2 제안 시스템 구성도

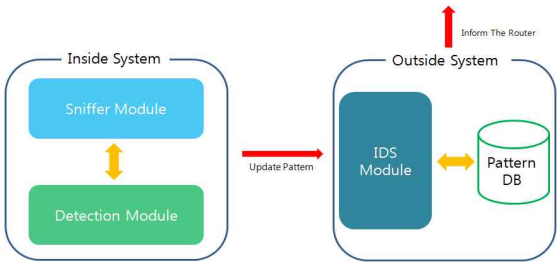
제안 시스템의 구성도는 [그림 5]와 같으며 라우터 뒷단에 Outside System(IDS)을 구성하고 로컬 네트웍에는 Inside System(Monitering)으로 구성된다. 모니터링 중Victim에서 의심스러운 메시지가 탐지되었다면 Inside System은 Outside System에서 False Negative가 일어났다고 판단하고 의심스러운 패턴을 Outside에게 쿼리를 날리고 Outside System에서는 업데이트를 수행함과 동시에 라우터에게 알려 주고 라우터는 의심되는 메시지의 목적지 주소를 차단하게 된다.



[그림 5] 제안 시스템 구성도

3.3 제안 시스템 구조도

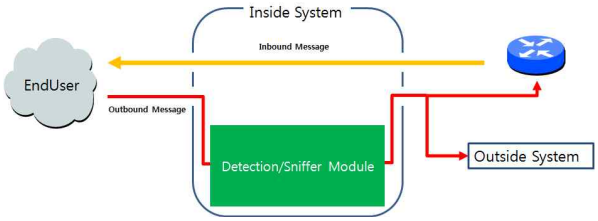
제안 시스템은 Inside System과 Outside System으로 구성되며 Inside System은 로컬 네트워크 즉 스위치 뒷단에 설치되며 설치되는 방식은 인라인 방식, 미러링 방식, 프록시 방식을 사용한다. Outside System은 IDS나 IPS같은 일반적인 네트워크 모니터링 및 탐지 차단을 수행하는 장비로 구성된다. 제안 시스템의 대한 구조도는 [그림 6]과 같으며 Inside System은 Sniffer Module과 Detection Module로 구성되며 Outside System은 일반적인 IDS구성 방식과 동일하다. Inside System은 BHO(Browser Helper Object)형식으로 설치되며 서버와 클라이언트 구조로 동작하게 된다. Inside System은 실시간으로 로컬네트워크에 모니터링을 수행하고 의심스러운 메시지를 탐지하면 즉각 Outside System에게 Update Pattern 쿼리를 전송하고 Outside System은 Pattern DB에 업데이트 수행함과 동시에 라우터에게 차단할 목적지 IP를 알려주고 라우터는 해당 IP로부터 들어오는 모든 패킷을 차단하도록 한다.



[그림 6] 제안 시스템 구조도

3.4 Inside System에서의 탐지 제안방법

Inside System에서 탐지하는 메시지는 [그림 7]과 같이 Outbound 트래픽에 대하여만 모니터링을 수행한다. 이는 EndUser에서 나가는 메시지를 탐지하기 때문에 Inbound 메시지를 탐지하는 것 보다 더 정확하게 판단이 가능하며, 또한 외부에서 내부로 유입되는 많은 메시지들에 대하여 네트워크에 대한 부하를 줄여준다. Outbound 메시지에 대하여 모니터링을 수행하고 의심되는 메시지일 경우에는, Outside System에게 알려주는 방법으로 진행되며, 일반적인 Outbound 메시지라고 한다면, 라우터에게 보내어 진다.

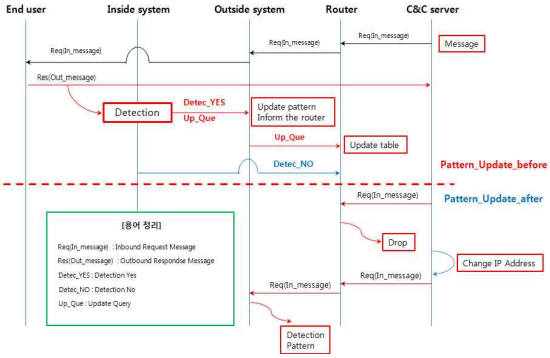


[그림 7] Inside System에서의 탐지 제안방법

3.5 제안 시스템 동작 절차

제안 시스템의 전체적인 동작구조는 [그림 8]같으며 Outside System에서는 False Negative가 일어났

다고 가정한다.



[그림 8] 제안 시스템 동작구조

C&C서버에서 EndUser에게 Req(In_message)메시지를 보내게 되면 라우터를 통과하여 IDS에서 False Negative가 발생되면서 내부로 메시지가 유입 된다.

이때, Inside System은 Inbound 메시지에 대해서는 탐지를 수행하지 않기 때문에 IDS를 통과하면 EndUser까지 넘어 가게 된다. C&C의 Req(In_message)를 받은 EndUser는 메시지에 대하여 응답하기 위해Res(Out_message)를 보내게 되는데 이때, Inside System은 EndUser에서 나가는 Outbound메시지에 대해서 모니터링을 수행하고 의심스러운 메시지라고 판단(Detec_YES)되면 곧바로 Outside System에게 (Up_Que)업데이트 쿼리를 날리고 Outside System은 해당 쿼리를 업데이트 함과 동시에 라우터에게 알려준다.

라우터와 Outside System에서의 업데이트가 끝난 후에C&C 서버에서는 EndUser에게 다시 Req(In_message)를 보내게 된다고 할지라도 라우터에서 차단리스트에 포함되어진 IP이므로 차단하게 되고, 다른 C&C서버를 이용하여 라우터를 통과 했다고 할지라도 Outside System에 등록된 패턴에 탐지가 되므로 역시 다른 IP를 이용하는 C&C서버 또한 IDS에서 탐지가 됨으로써 C&C서버와 EndUser 사이의 연결을 차단하여 봇넷이 형성되지 못하도록 한다. 또한 IDS에서 탐지된 IP는 라우터에게 알려줌으로써 C&C서버가 많이 사용되는 네트웍 대역을 파악 할 수 있다. 만약 EndUser에서 나가는 메시지가 일반적인 메시지라고 한다면 일반적인 통신상의 메시지가 흘러가는 방식으로 진행된다.

4. 결론 및 향후 연구과제

DDoS공격은 점점 더 발전하고 있으며 예전의 독립적인 프로토콜을 사용하던 구조에서 일반적인 프로토콜을 사용 하는 흐름으로 넘어 오면서 프로토콜의 상의 취약성을 이용한 DDoS공격이 많이 발생하고 있다. 구성방식도 IRC, P2P, HTTP 등 많은 종류의 방식을 사용하고 있으며 예전의 전체 네트웍에 대하여 엄청난 트래픽을 발생시키는 구조에서 어플리케이션 자체에 대한 공격 등 공격 형태도 점점 다양해지고 있는 실정이다. 이러한 공격은 네트웍에 대한 통계적인 방법으로는 탐지가 불가능하고 패턴 기반의 시그니처를 이용하는 방법으로도 한계가 있기 때문에 수동적 네트워크 탐지 방법론보다는 실시간으로 처리 할 수 있는 능동적 네트워크 탐지 방법론에 대한 연구가 절실하게 요구된다.

본 논문에서 제안한 시스템을 실시간으로 동작시키기 위한 연구가 필요하며 Inside System에서 탐지하는 방법론에 대한 연구가 절실히 요구된다. 본 논문은 DDoS를 탐지하기 위한 능동적 네트워크 방법론에 대하여 말하고 있으며, Inside System에서의 탐지 알고리즘 부분에 대하여 많은 테스트를 병행하여야 한다. 추후에는 P2P기반을 이용한 DDoS 탐지 방법도 연구할 예정에 있다.

참고문헌

[1] Peng, T, 외 2인, “Survey of Network-based Defense MechanismsCountering the DoS and DDoS Problems”, *ACM Comput. Surv.* 39, 1, Article 3, April 2007.

[2] Stephen M. Specht, Ruby B. Lee "Distributed Denial of Service: Taxonomies of Attacks, Tools and Countermeasures", *2004 International Workshop on Security in Parallel and Distributed Systems, pp. 543-550, September 2004.*

[3] Jelena Mirkovic, Peter Reiher, “A Taxonomy of DDoS Attack and DDoS Defense Mechanisms”, *ACM SIGCOMM Computer Communication Review*, Volume 34, Issue 2, pp. 39-53, April 2004.

[4] 구자현 "서비스 거부 공격의 유형 및 대응" 주간기술동향 통권 1337호 2008. 12. 17.

[5] 최양서(Choi Yang-Seo) 외 “분산서비스거부 공격 통합 대응체계 연구” 정보보호학회지 제19권 제5호, 2009. 10.

[6] RFC2616, "Hypertext Transfer Protocol -HTTP /1.1"