액티브 네트워크 기반의 분산 서비스 거부 공격 대응 메커니즘

김현주, 나중찬, 손승원

한국전자통신연구원, 네트워크 보안 연구부

Active Response Mechanism to Distributed Denial of Service Attack on Active Networks

Hyun Joo Kim, Jung-chan Na, Sung-won Sohn

Department of Network Security, Electronics and Telecommunications Research Institute(ETRI)

요 약

기존의 네트워크 보안은 침입 징후를 탐지하여 외부 공격자로부터 오는 트래픽을 차단함으로써 자신의 도메인만을 보호하였다. 이는 공격자로 하여금 제 2, 제 3의 공격을 가능하게 하고 공격자에 대한 대응에 있어서도 각 도메인간의 협력이 없는 상태를 야기하였다. 따라서 각 도메인 간의 데이터의 상호 결합과 협력을 통해 공격자의 실제 위치를 추적하여 침입 근원지로부터의 트래픽을 차단함으로써 공격자를 네트워크로부터 고립시키고자 하는 연구가 진행되고 있지만, 이는 분산서비스거부 공격의 경우 제한적이다. 그리므로 본 논문은 분산서비스거부 공격에 있어 에이전트와 마스터의 위치를 추적하여 제거하고 실제 공격자를 고립시킬 수 대응 메커니즘에 대해 논의한다.

I. 서론

기존의 네트워크 보안은 침입 징후를 탐지하여 외부 공격자로부터 오는 트래픽을 차단함으로써 자신의 도메인만을 보호하였다. 하지만 이러한 경우 공격자는 아무런 제약없이 인터넷을 자유로이 이용할 수 있어 제 2, 제 3의 공격을 시도하게 된다. 또한 동일한 공격에 대해서 전체 네트워크의 다른 부분에서 인식하게 되는 정보와 전체 네트워크 차원에서 해당 데이터를 상호 결합하는 기능이 부족하고, 공격자에 대한 대응에 있어서도 각 도메인간의 협력이 없는 상태이다. 따라서 전체 네트워크를 구성하는 각 도메인간의 데이터의 상호 결합과 협력을 통해 공격자의 실제 위치를 추적하여 침입 근원지로부터의 트래픽을 차단함으로써 공격자를 네트워크로부터 고립시키고자 하는 연구가 진행되고 있다. 이와 관련된 대표적인 연구는 DARPA(Defense Advanced Research Project Agency) 프로젝트인 IDIP(Intrusion Detection Isolation Protocol) [1]와 이를 보완한 AN-IDR [2][5]를 들 수 있다. 그러나 AN-IDR은 분산서비스거부(Distributed Denial of Service: DDOS) 공격 대응 메커니즘의 범위를 에이전트로 한정하고 있다. DDOS 에이전트로부터 발생하는 트래픽을 일단 차단하고 숙주로서 사용되는 에이전트 프로그램을 제거한 후 차단을 해제하는 방식으로 대응을 하고 있다. 즉 실제 공격자를 네트워크로부터 고립시키는 것이 아니라 DDOS 공격을 위해 이용되는 에이전트만을 제거하는 것만을 언급하고 있다. 따라서 본 논문에서는 DDOS 공격에 있어 에이전트와 마스터의 위치를 추적하여 제거하고 실제 공격자를 고립시킬 수 있는 센서들을 정의하고 DDOS 공격을 보다 능동적으로 대응할 수 있는 대응 메커니즘을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서 AN-IDR에 관하여 간략하게 소개하고 3장에서는 액티브 네트워크 기반의 분산 서비스 거부 공격의 대응 메커니즘에 대해 논의한다. 마지막 4장에서는 결론 및 향후 계획을 기술한다.

II. 관련 연구

본 장에서는 DDOS 공격을 대응하기 위한 관련 연구로서 DARPA의 AN-IDR에 대해여 살펴본다.

1. AN-IDR

AN-IDR(Active Network- Intrusion Detection and Response)은 DARPA 프로젝트로 기존의 네트워크 보안 기술의 한계와 DARPA의 SLSS(Survivability of Large Scale System) 프로그램의 하나로 연구된 IDIP를 보완한 것이다. AN-IDR은 IDIP 구조를 그대로 적용하고 보안상 관리 도메인을 계층적인 구조로 가짐으로써 공격자의 추적 및 대응을 용이하게 하였다. 또한 TCP, UDP 등을 통한 공격을 탐지하고 각 라우터에서 모니터링한 정보를 토대로 액티브 패킷을 이용하여 역추적을 수행하여 공격자를 고립시키는 메커니즘을 제공하고 있다.

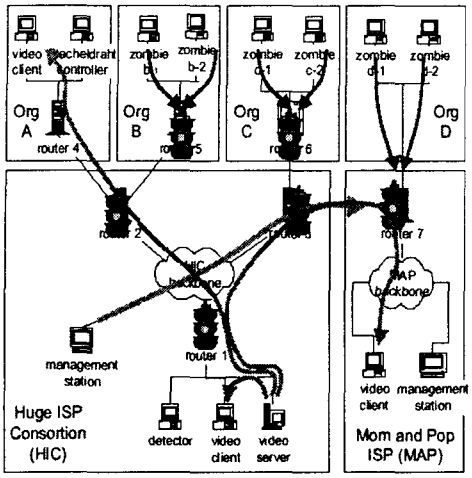

그림 1. AN-IDR에서의 DDOS 대응

그림 1은 AN-IDR에서의 DDOS 공격 대응 방법을 도식화한 것으로 Org B, C, D에 존재하는 zombie들이 HIC내의 비디오 서버에 DDOS 공격을 수행하여 비디오 클라이언트로 서비스를 제공하는 것을 방해한다. 각 도메인은 협력관계를 유지하며 공격이 탐지되면 detector가 라우터 1, 2, 3에게 IDIP traceback을 전송한다. 이를 받은 라우터들은 HIC 관리스테이션에 자신이 공격 ingress point임을 알리면 관리 스테이션은 active rate limiter를 라우터 1에 파송하여 공격지로부터 유입되는 패킷을 일차적으로 차단한다. 이후 라우터 1에 파송된 rate limiter가 라우터 2, 3으로 이동하여 위와 과정을 반복하여 DDOS 공격에 사용되는 zombie 호스트들을 고립시킴으로써 정상적인 서비스를 가능하게 한다.

이는 현재의 DDOS 공격에 이용되는 zombie만을 제거했을 뿐 실제 공격자에 대한 대응이 이루어지지 않아 제2, 제 3의 공격 기회를 제공한다.

III. 액티브 네트워크 기반의 DDOS 공격 대응 메커니즘

본 장에서는 액티브 네트워크[3] 상에서 DDOS 공격 대응을 수행하는 능동 보안 시스템의 구조와 이에 사용되는 각각의 센서를 정의하고 DDOS 마스터와 실제 공격자에 대해서도 대응할 수 있는 메커니즘에 대하여 논의한다.

1. 능동 보안 시스템의 전체 구조

능동 보안 시스템(Active Security System)은 액티브 네트워크 기반의 침입 탐지 및 대응 시스템으로 TCP 우회 공격과 Spoofed IP 공격에 대해 세션 정보와 MAC 주소 등을 이용한 역추적을 수행하여 공격자를 고립시키고 도메인 내의 관리 시스템들 간의 협력을 통해 능동적이고 보다 강력한 대응을 수행한다. 본 논문에서는 이러한 능동 보안 시스템을 통해 DDOS 공격을 보다 본질적으로 대응할 수 있는 부분에 대해서만 설명한다.

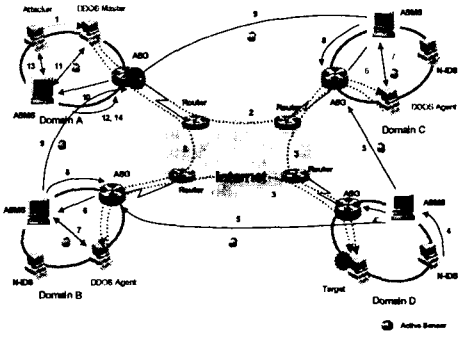

그림 2. 능동 보안 시스템의 네트워크 구조

그림 2는 능동 보안 시스템의 네트워크 구조로 DDOS 공격 대응 시나리오를 도식화한 것이다.

능동 보안 시스템은 각 도메인을 관리 통제하는 ASMS(Active Security Management System), 각 도메인의 경계에 위치하여 각각의 센서를 수행하고 라우터의 기능을 담당하는 ASG(Active Security Guard), 네트워크 기반의 침입탐지 시스템(N-IDS)과 액티브 센서들로 구성된다. 그림 2의 시나리오에 대한 자세한 설명은 다음 2절의 대응 메커니즘의 순서도를 통해서 단계별로 알아본다.

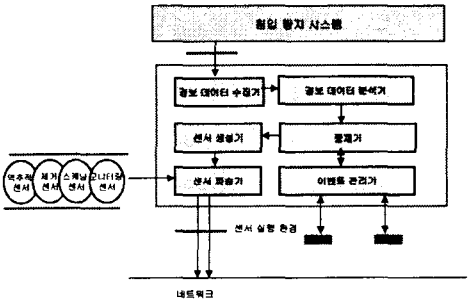

그림 3. ASMS의 구조

그림 3은 ASMS의 구조를 단순화하여 표현한 것으로 네트워크 기반의 침입탐지 시스템으로부터 경보 데이터를 수집하는 경보 데이터 수집기와 수신된 경보 데이터를 판단하고 역추적에 필요한 데이터를 추출하는 경보 데이터 분석기, 추출된 정보를 기반으로 역추적 센서를 생성하는 센서 생성기와 해당 경보 데이터로부터 추출한

근원지 IP 주소로 센서를 파송하는 센서 파송기로 구성된다. 또한 여러가지 액티브 센서들이 존재하며 ASMS내의 여러 구성 요소들을 통제하는 중재기 및 센서 실행 메시지를 수신하는 이벤트 관리기로 이루어진다.

다음은 각 센서들의 기능에 대해 나열한다.

■ 역추적 센서: 각 도메인 경계의 ASG에 파송되어 경보 데이터로부터 검출된 해당 IP를 차단한다.

■ 스캐닝 센서: 역추적 대상 호스트에 설치된 에이전트나 마스터 프로그램을 찾아내기 위한 것으로 기존의 DDOS 공격의 다양한 유형에 따라 스캐닝한다. 새로운 DDOS 유형이 추가되면 그 모듈만을 업데이트하여 스캐닝 센서를 유지한다.

■ 제거 센서: 검출된 DDOS 에이전트와 마스터 프로그램을 삭제한다.

■ 모니터링 센서: 다음 단계의 역추적 과정을 진행하기 위해 삭제된 프로그램으로 접근하는 패킷들을 감시한다.

2. 능동 보안 시스템의 DDOS 대응 메커니즘

설명에 앞서 능동 보안 시스템의 DDOS 대응 메커니즘은 DDOS 공격에 있어 공격자가 마스터를 통해 에이전트에 재접속을 시도한다는 것을 가정하고 있다. 이는 숙주로 사용되는 마스터와 에이전트는 보안 홀로써 충분히 재사용 되어 제 2, 제 3의 공격에 이용될 수 있기 때문이다. 아래 그림 4는 DDOS 공격 대응 메커니즘의 순서도이다.

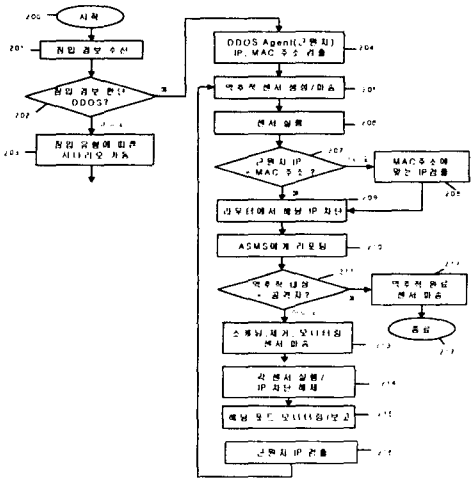

그림 4. DDOS 공격 대응 메커니즘의 순서도

DDOS 공격 대응 메커니즘은 3단계의 역추적 과정으로 이루어진다. <그림 4 참조>

1) 제 1 단계 역추적 과정

제 1단계 역추적 과정은 에이전트를 찾아내어 제거하는 과정으로, 먼저 ASMS는 N-IDS으로부터 침입 경보 데이터를 수집(201)한다. 침입 경보 데이터를 통해 침입 유형이 DDOS 공격인지를 확인(202)하고 DDOS 공격이 아닌 경우 침입 유형에 따른 대응 시나리오가 가동(203)된다. 만약 DDOS 공격인 경우, ASMS는 서비스거부 공격의 패킷들의 근원지 IP 주소와 MAC주소를 검출(204)한다. 이는 우선 DDOS 공격 에이전트가 설치된 위치로 판단할 수 있다. 주소를 검출한 후 DDOS 공격의 숙주로 이용되고 있는 에이전트를 제거하기 위해 역추적 센서를 생성하여 파송(205)한다. 이렇게 파송된 센서는 에이전트가 위치된 도메인 경계에 위치한 ASG로 수신되어 실행(206)된다<그림 2의 5>. 이 때 역추적 센서 내에 포함된 근원지 IP주소가 ASG가 가지고 있는 매핑 테이블에 기록된 MAC 주소와 일치하지 않는다면 이는 위조된 IP주소로 공격이 이루어진 것이므로 ASG는 센서 내에 포함된 MAC주소를 바탕으로 실제 에이전트의 위치를 판단하여 해당 IP주소로부터 생성된 트래픽을 차단(209) 한다.

ASG는 위와 같이 센서를 실행한 후 트래픽 차단이나 해제 등의 이벤트를 ASMS에게 보고(210)한다. 센서 실행에 대한 결과를 통보 받은 ASMS는 역추적 대상이 실제 공격자인지를 판단한 후 공격자가 아닌 DDOS 공격의 에이전트를 추적하는 단계이므로 에이전트 프로그램을 삭제하기 위해 역추적 대상 호스트로 스캐닝, 제거, 모니터링 센서를 파송(213)한다. 센서들의 수행으로 에이전트프로그램이 완전히 제거된 후 트래픽 차단을 해제(214)한다. 이는 에이전트와 마스터도 공격에 이용당한 피해자이므로 네트워크를 자유롭게 사용할 수 있게 해 주어야 하기 때문이다. 모니터링 센서는 에이전트나 마스터 프로그램이 사용하는 포트로 접근하는 패킷이 검출된 경우 이를 ASMS에게 통보(215)한다. ASMS는 통보 받은 패킷의 근원지 IP 주소를 검출(216)하여 다음 단계의 역추적 과정을 수행한다.

2) 제 2 단계 역추적 과정

제 2단계 역추적 과정은 마스터 프로그램을 제거하는 과정으로, 제 1단계에서 검출된 패킷 근원지 IP 주소를 토대로 하여 마스터 역추적 과정이 진행된다. 그림 4의 205번부터 다시 수행되는 것으로 마스터가 설치된 호스트로 역추적 센서를 생성하여 파송하는 것을 시작으로 제 1단계의 과정을 반복한다. 이 때 그림 2의 9처럼 한 ASG에 동일한 IP를 역추적하기 위한 센서가 수신된다면 ASG는 뒤에 수신된 센서를 무시한다. 제 2단계에서는 공격자의 IP주소를 검출하기 위해 마스터 프로그램을 제거한 후 이에 접근하는 패킷을 모니터링하게 된다. 모니터링 센서로부터 보고된 패

킷의 근원지 IP 주소가 실제 공격자의 위치가 되며 실제 공격자를 네트워크로부터 고립시키기 위해 제 3 단계의 역추적 과정이 수행된다.

3) 제 3 단계 역추적 과정

제 3단계 역추적 과정은 공격자 호스트를 네트워크로부터 고립시키는 과정으로, 제 1, 2 단계와 같이 205번부터 210번 과정을 거친 후, 211번 과정에서 역추적 대상이 공격자이고 209번 과정에서 공격자의 IP 로부터 생성되는 트래픽을 차단하였으므로 공격자는 네트워크로부터 고립된다. 따라서 역추적 완료 메시지를 ASMS에게 전송함으로써 DDOS 공격 대응을 종료한다.

이와 같은 세 단계의 과정을 거치게 되면 에이전트와 마스터는 정상적으로 네트워크를 사용할 수 있게 되고 공격자만이 네트워크로부터 고립되어 제 2, 제 3의 공격을 방지할 수 있다.

IV. 결론 및 향후 계획

기존의 네트워크 보안은 침입 징후를 탐지하여 외부 공격자로부터 오는 트래픽을 차단함으로써 자신의 도메인만을 보호하였으므로 이러한 경우 공격자는 아무런 제약없이 인터넷을 자유로이 이용하여 제 2, 제 3의 공격을 시도하게 된다. 따라서 자신의 도메인만을 보호하는 것이 아니라 공격자를 네트워크로부터 고립시키고자 역추적 시스템에 관한 연구가 계속되고 있고 역추적 기법을 이용한 DDOS 공격 대응 기술에 대한 관심도 증가하고 있다. 하지만 DDOS 공격 대응 메커니즘에 관한 연구 [4]는 아직 정형화된 것이 존재하지 않으며, DDOS 에이전트의 위치를 파악하여 패킷을 차단하고 DDOS에이전트 프로그램을 제거하여 숙주로써 이용당한 시스템을 복구하는데 그치고 있다.

그러므로 본 논문에서는 DDOS에이전트를 제거하는 것뿐만 아니라 에이전트와 마스터 프로그램을 제거하여 해당 호스트가 정상적으로 네트워크를 이용할 수 있도록 복구하고 실제 공격자만을 네트워크로부터 고립시킬 수 있는 DDOS 대응 메커니즘을 제안하였다. 본 메커니즘은 공격 당시 에이전트로부터 발생하는 공격 패킷을 차단함으로써 일차적인 대응을 수행하고 향후 제2, 제3의 공격을 방지하기 위해 마스터와 실제 공격자를 역추적한다. DDOS 공격의 공격자는 마스터와 에이전트를 그 시스템의 보안 홀로써 사용하기 때문에 차후 재접속을 시도한다. 그러나 만약 실제 공격자가 다시 마스터로 재접속을 시도하지 않는다면 본 메커니즘에 추가적으로 각 호스트마다의 세션 로깅 기능을 부여하여야 한다. 하지만 이에 대한 각 호스트들의 과부하 및 성능에 대한 고려가 필요하며, 향후 ASG 내의 매핑 테이블의 관리에 대한 추가적인 연구도 요구된다.

참고문헌

[1] D. Schnackenberg, K. Djahandari, and D. Sterne, "Infrastructure for Intrusion Detection and Response", *Proceedings of the DARPA Information Survivability Conference and Exposition*, Jan. 2000.

[2] D. Sterne, D. Schnackenberg, and etc., " Autonomic Response to Distributed Denial of Service Attacks", *Proceedings of the Recent Advances in Intrusion Detection (RAID) 2001 conference*, 2001.

[3] S. Bhattacharjee, K.L. Calvert and E.W. Zegura, "An Architecture for Active Networking", *High Performance Networking (HPN'97)*, White Plains, NY, April 1997.

[4] Stamatis Karnouskos, "Dealing with Denial of Service Attacks in Agent-enabled Active and Programmable Infrastructures", *Proceedings of the 25th Annual International Software and Application Conference(COMPSAC01)*, 2001.

[5]http://www.nai.com/research/nailabs/adaptive-network/active-networks.asp