분산 서비스거부 도구들의 위상 탐지를 위한 분산 탐지 기법

정유석° 홍만표
아주대학교 정보통신전문대학원
{j8508°, mphong}@ajou.ac.kr

Detection Method for Finding Topology of DDoS Tools

Yoosuk Jung° Manpyo Hong
Graduate school of Information and Communication, Ajou University

요 약

인터넷 발전의 대표적인 역기능인 시스템 공격 방법 중 분산 서비스거부 공격은 공격 도구가 분산되어 있고 도구를 분산화 하는 과정을 찾기 힘들다는 특징 때문에 현재까지의 연구 대부분에서 공격이 발생한 시점에서의 대응 방법이 제안됐다. 그러나 이 시점에서의 대응은 시스템에 대한 보호가 늦어질 가능성이 높기 때문에, 공격이 발생되기 이전에 네트워크 상의 패킷의 흐름을 거시적으로 판단해서 공격의 징후를 찾고 이에 대해 대처할 수 있는 방법이 필요하다.

따라서 본 논문에서는 분산화 된 보안 에이전트들에 의해 공격 시점 이전에 분산 서비스거부 공격 도구의 위상을 탐지하는 기법을 제안한다. 이 기법은 분산된 공격 도구에서 발생할 수 있는 의심스러운 접속들을 포괄적으로 판단하여 공격이 발생하기 전에 공격도구들이 설치된 위치를 찾게 된다.

1. 서론

최근 정보통신기술의 비약적인 발전과 제반 환경의 보급은 인터넷 기반의 새로운 시장과 문화를 창출할 뿐 아니라 기존 산업사회 전반을 정보사회로 변화시키고 있는 등 인간의 삶을 더욱 풍요롭게 하는데 일조를 하고 있다. 그러나 이와 같은 긍정적인 측면의 증가와 함께 개인 정보의 유출, 시스템의 오·남용, 인터넷을 통한 전산망 해킹 등 매우 위험하고 파괴적인 역기능의 문제 또한 발생하고 있는데, 이는 정보화가 진전될수록 더욱 확대되는 양상을 보이고 있으며, 그 피해 정도 또한 갈수록 심각해지고 있다.

그 중 2000년 초 Yahoo, CNN등의 대형 웹 페이지에 대한 공격 사건으로 널리 알려진 분산 서비스거부 공격(distributed denial of service : DDoS)은, 인터넷 상의 불특정 다수의 호스트에 단일 공격자에 의한 공격도구가 설치된 후, 공격자가 원하는 시점에 목표 서버를 동시에 공격하여 수행된다. 그런데 공격을 위한 도구가 분산되어 있고 도구를 분산화 하는 과정을 찾기 힘들다는 특징 때문에 현재까지 연구된 탐지 방법들은 공격이 발생되는 시점에야 탐지가 가능하며 이때는 이미 공격에 대한 대처를 하기에 늦을 가능성이 높다. 따라서 공격이 발생되기 이전에 네트워크 상의 패킷의 흐름을 거시적으로 판단해서 공격의 징후를 찾고 이에 대해 대처할 수 있는 방법이 필요하다.

따라서 본 논문에서는 분산 서비스거부 공격의 사전탐지를 위한 방법을 제안한다. 이를 위해 네트워크 상에 분산된 보안 에이전트들이 공격과 관련된 정보를 수집·교환하여 공격 지도 후보를 작성하고 이로부터 공격 위상을 탐지하는 방법을 제안한다.

2. 관련연구

기존의 분산 서비스거부 공격에 대처하기 위한 연구는 공격이 발생하는 시점에 이를 탐지하고 대처하는 것에 초점이 맞추어져 있다.

Park[1]은 라우터를 기반으로 한 필터링을 통해 분산 서비스거부 공격을 해결하고자 했다. 각 라우터에서는 라우팅 및 네트워크 망 정보를 통해 필터링 테이블을 작성한 후, 패킷의 도착지 주소와 목적지 주소를 통해 정당성을 판단하여 패킷을 걸러내는 작업을 수행한다. 패킷의 필터링은 네트워크 전체에 걸쳐 발생 되 공격 목표보다 훨씬 이전에 공격 패킷을 차단할 수 있다. 그러나 패킷의 필터링 시점 이전에 공격 대상이 마비될 수도 있고, 정상적인 패킷이 필터링 되어 결과적으로 방어에 의한 서비스 거부가 발생할 수도 있는 문제가 있다.

Chen[2]은 기존의 분산 서비스거부 공격을 방어하기 위한 방법인 게이트웨이 라우터들에서의 트래픽 형상화를 개선해서 기존 방안의 단점인 게이트웨이의 과부하, 네트워크의 대역폭의 소모, 악의적인 패킷의 비 처리 등을 극복했다. 이를 위해 능동 네트워크 패러다임을 채택했으며, 네트워크 구성을 위해 능동 노드들을 사용해 거기에 설치된 능동 컴퍼넌트에 의해 공격을 탐지하고 대응한다. 그런데 이 방법 또한 공격이 발생되는 시점에

패킷의 량을 측정하여 공격을 탐지하므로 공격에 대한 대처보다 공격 대상의 마비가 먼저 발생할 수 있다.

AT&T에서 제안한 푸시백(pushback)[3] 기법은 공격 트래픽으로부터 공격 패킷의 특정 패턴을 정의한 후 정보 메시지를 상위 라우터로 푸시백 시켜서 상위 라우터 상에서 필터링 시킨다는 것이다. 이 기법은 분산 서비스 거부 공격이 일어날 때 공격 대상자 주위의 패킷의 밀집 정도를 통해 공격을 탐지한다. 그러나 시그니쳐 생성의 대상이 패킷의 목적 주소로만 이루어져 있어 이에 대한 개선이 필요하며, 위의 연구들과 마찬가지로 실제 공격이 발생하는 시점에 공격에 대한 탐지과정이 수행되므로 공격에 대한 대처보다 공격 목표의 마비가 먼저 발생할 수 있다.

3. 분산 서비스거부 공격의 특성

현재의 기술로는 분산 서비스거부 공격이 발생되기 이전에 이와 관련된 도구들을 탐지하는 것은 매우 어렵다. 그 이유로 도구들을 탐지하는데 필요한 정보, 즉 도구들에 의해 발생되는 이벤트나 패킷들에 대한 연구가 부족하며, 게다가 단일 도구에서 발생되는 단편적인 패킷들만으로는 정상적인 패킷과의 구분이 매우 어렵기 때문이다. 따라서 단편적인 패킷을 통한 정상적인 프로그램 혹은 호스트와의 구분이 아니라 거시적인 통신 흐름을 통한 공격 도구들의 탐지가 필요하다. 다음은 이와 관련된 도구들의 행동 특성이다.

분산 서비스거부 공격 도구들은 다음과 같은 일련의 과정을 거친다. 탐색(proving), 설치(implant), 확인(confirm), 공격(attack)의 4단계가 그것으로 탐색 단계에서는 공격도구 설치를 위한 대상을 탐색하며, 설치 단계에서는 선정된 대상에 대해 공격 도구를 설치하고, 확인 과정에서 공격에 필요한 각종 설정을 하고, 마지막으로 공격 단계에서 공격 목표에 향한 대규모의 패킷을 생성한다. 그런데 위의 단계 중 탐색, 설치, 확인의 과정에서 공격 도구들은 각 작업을 위한 패킷을 발생시키며, 이 정보들은 단편적으로 정상일 수 있으나, 거시적 측면에서 전체 패킷의 형상을 살필 경우 비정상적인 흐름임을 알 수 있다. 따라서 본 논문에서는 이러한 특성을 이용해 분산 서비스거부 공격 도구를 탐지하고자 한다.

4. 분산 탐지 기법

4.1 개요

제안하는 기법은 분산 서비스거부 공격이 발생하기 이전에 공격 도구의 위상을 탐지한다. 이를 위해 네트워크 상에 분산화 되어 배치된 보안 에이전트들이 네트워크 상의 호스트들의 통신을 감시하고, 공격 도구의 행위로 의심되는 접속들로부터 공격 후보 그래프를 생성하여, 이를 통해 공격 도구들의 위상을 탐지한다. 이때 공격 도구의 위상을 탐지하기 위한 공격 후보 그래프는 모든 보안 에이전트들이 공유한다.

공격 도구 위상의 탐지 시나리오는 [그림 1]과 같다.

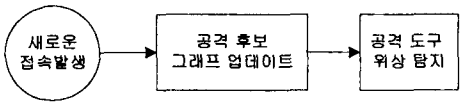

그림 1. 공격 위상 탐지 시나리오

4.2 공격 후보 그래프 업데이트

보안 에이전트는 새로운 접속이 발견되면 해당 접속이 의심스러운 접속(suspicious connection)인지 확인하고, 의심스러운 접속인 경우 관련된 정보로부터 공격 후보 그래프를 이루는 간선(candidate pair : CP)을 변경하여 공격 후보 그래프를 업데이트 한다. 이때 의심스러운 접속은 공격 도구로부터 파생될 수 있는 모든 종류의 접속을 의미하며, 그 예로 탐색 단계에서 나타날 수 있는 닫혀진 포트에 대한 접속 시도가 있다. 공격 후보 그래프의 간선은 특정 호스트간에 발생된 의심스러운 접속의 종류 및 횟수의 정보를 포함하며 다음과 같이 표현한다.

$$CP_{(s,d)} = \{ t_1^{a1}, t_2^{a2}, \cdots, t_n^{an} \} ,$$

s : 근원 호스트, d : 목적 호스트, tn : 접속 종류, an : 발생 빈도

이 정보는 추후 공격 도구의 위상을 탐지하기 위해 사용되는데, t_n은 두 호스트간에 그전에 발생하지 않던 새로운 종류의 접속이 발생한 경우 추가되며, a_n은 두 호스트간에 이미 발생되었던 종류의 접속이 발생한 경우 증가시킨다.

4.3 공격도구 위상 탐지

공격도구의 위상은 보안 에이전트들에 의해 생성된 공격 후보 그래프를 통해 판단한다. 공격 후보 그래프 중 동일 호스트로부터 파생된 부그래프를 하나의 공격 후보군으로 판단하여 다음에 정의되는 3가지 임계값에 의해 해당 공격 후보 군이 공격도구의 위상임을 판별한다.

- wthr(weight threshold) : 공격 후보 그래프의 간선을 공격도구 간의 통신이라고 판단할 수 있는 기준. 접속 종류와 횟수로 계산한다. 이때 wthr을 초과하는 간선의 자식노드를 유효자식이라고 명한다.
- cthr(children threshold) : 공격 후보 그래프의 노드의 공격도구의 중간자로 여길 수 있는 유효 자식 수의 정도. 이때 cthr을 초과하는 자식을 갖는 노드를 유효부모라고 명한다.
- pthr(parent threshold) : 공격 후보 그래프를 공격 도구의 위상으로 여길 수 있는 유효부모의 수.

wthr은 공격 도구간의 접속이 단일횟수로 끝나지 않는다는 특성으로부터, cthr은 공격 도구의 특성상 단일 노드로부터 다량의 자식노드가 생산된다는 특성으로부터,

마지막으로 pthr은 다량의 자식노드를 생성하는 노드가 다수 존재한다는 특성으로부터 정의되었다.

공격도구의 위상 탐지 시점은 의심스러운 접속이 발생했을 시점이며, 이때 의심스러운 접속이 포함되는 공격 후보 군에 대한 공격 위상 탐지를 수행한다.

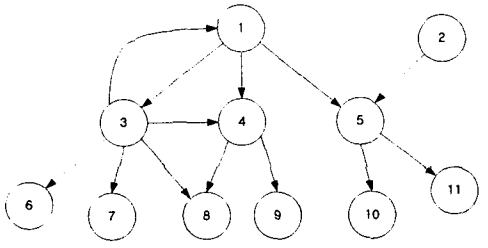

그림 2. 공격 그래프 후보의 예

예를 들어 [그림 2]와 같은 공격 그래프 후보가 존재하고 wthr = 1, cthr = 1, pthr = 2라고 할 때, 공격 후보 군은 1이나 3을 근원으로 하는 부그래프와 2를 근원으로 하는 부그래프로 나타난다. 이때 먼저의 후보 군은 유효부모가 1, 3, 4, 5의 4개이며 다른 후보군은 5의 1개이다. 따라서 1이나 3을 근원으로 하는 공격 후보 군은 공격 도구의 위상이라 할 수 있다.

5. 모델 분석

제안된 기법은 의심스러운 접속에 대한 정의, 공격 후보 그래프의 작성 및 표현 방법, 공격도구 위상 탐지를 위한 3가지 임계값의 결정에 따라 다양한 결과를 나타낼 수 있다. 그 중 의심스러운 접속에 대한 정의는 분산 서비스거부 공격 도구의 행동 특성의 분석과 밀접한 관련이 있으며, 따라서 의심의 대상이 되는 접속의 범위 및 정확성에 영향을 준다. 공격 후보 그래프의 작성 및 표현 방법의 정의는 네트워크 상에서 실시간으로 공격 도구들의 위상을 탐지하는데 사용됨으로 실제로 위상 탐지에 필요한 시간을 결정하는 요소이다. 마지막으로 3가지 임계값의 결정은 분산 서비스거부 공격 도구들의 위상적 특성과 밀접한 관계가 있으며 결과적으로 탐지된 위상에 대한 정확성과 관련이 있다.

6. 결론 및 향후과제

본 논문에서는 분산화 된 에이전트들에 의해 분산 서비스거부 공격 도구의 위상을 탐지하는 기법을 제안했다. 이를 위해 공격 위상 탐지 시나리오와, 의심스러운 접속들의 그래프 화, 그리고 그래프를 바탕으로 한 공격 도구의 위상탐지 방법을 제안했다. 제안된 기법은 분산된 보안 에이전트를 통해 공격 도구에서 발생할 수 있는 의심스러운 접속들을 포괄적으로 판단하여 공격이 발생하기 전에 공격도구들이 설치된 위치를 찾는다는 것에 의의가 있다. 그러나 이를 수행하는 보안 에이전트들의 구체적인 작동 방법의 고안과, 위상 탐지를 위한 최적화 방안의 제안 그리고 공격 그래프 후보의 유지 시간 고려 등의 추가적인 연구가 필요하다.

7. 참고문헌

[1] Kihong Park, Heejo Lee, "On the Effectiveness of Route-Based Packet Filtering for Distributed DoS Attack Prevention in Power-Law Internets," *Proc. ACM SIGCOMM*, 2001

[2] Chen, E.Y., Fuji, H.; Kashiwa, D., "Active Shaping : A Countermeasure against DDoS Attack," *EDUMN 2002. 2nd European Conference on*, 2002

[3] John Ioannidis, Steven M. Bellovin , "Implementing PUSHBACK" , *AT&T labs Research* , 2002

[4] Kalman K. K. and Rocky K. C. Chang, "Engineering of a Global Defense Infrastructure for DDOS Attacks," *ICON 2002. 10th IEEE International Conference on*, 2002. Page(s): 419-427

[5] Xianjun Geng and Andrew B. Whinston, "Defeating Distributed Denial of Service Attacks", *IT Professional*, Volume: 2 Issue: 4, July-Aug. 2000

[6] Phillip A. Porras and Peter G. Neumann, "EMERALD: Event Monitor ing Enabling Responses to Anomalous Live Disturbances", *1997 National Information Systems Security Conference*, pp.353-365, October 1997.

[7] S. Staniford-Chen, S. Cheung, R. Crawford, M. Dilger, J. Frank, J. Hoagland, K. Levitt, C. Wee, R. Yip, D. Zerkle, "GrIDS -- A Graph-Based Intrusion Detection System for Large Networks", 1996.