라우터간의 상호 협조를 통한 보안 프로토콜의 개발

김용재*, 김한규*
*홍익대학교 대학원 전자계산학과
e-mail:{kimyj, khim}@cs.hongik.ac.kr

Development of Security Protocol with Router Cooperation

Yong-Jae Kim*, Han-Kyoo Kim*
*Hongik Univ. Dept. of Computer Science

요약

한 호스트에게 과다한 트래픽을 보내는 서비스 거부 공격을 막기 위하여, 허용한도 이상의 트래픽을 차단할 필요가 있다. 이 때 가능한 한 트래픽의 근거지에서 가까운 곳의 라우터에서 그 차단을 실행해 줄수록 이상적으로 차단할 수 있으므로, 공격자의 네트워크 상의 위치를 파악하는 일이 중요하다. 본 연구에서는 피해자의 요청 및 공격의 파악에 따라, 피해자와 공격자사이에 있는 공격경로 상의 라우터들이 서로 협조하여 공격자를 적발할 수 있는 프로토콜을 제안한다. 설계된 프로토콜은 시뮬레이션을 통하여 성능을 평가하였으며, 그 결과 설계된 프로토콜은 적은 시간 내에 공격자의 위치를 찾는 효과를 가져왔다.

1. 서론

인터넷에 대한 수요는 계속 폭발적으로 증가하고 있으며, 그에 따른 보안의 중요성 역시 대두되고 있고, 보안 및 네트워크 운용에 악영향을 주게 되는 악의적인 공격도 따라서 증가해왔다. 대표적인 공격중 하나인 서비스 거부 공격[1]은, 처리능력 이상의 과도한 양의 패켓을 호스트에게 전달하는 방법으로 수행된다.

본 논문에서는 공격자와 피해자 사이에 존재하는 라우터들의 상호 협조를 통하여 공격자를 추적하고, 그의 공격을 차단하는 방식을 설명하고, 나아가 공격자의 공격을 차단하는 방법을 제안하며, 그 시스템 구성을 설명한다.

성능 분석을 위한 시뮬레이션으로는 캘리포니아대학에서 개발한 NS 네트워크 시뮬레이터를 이용하였다[5].

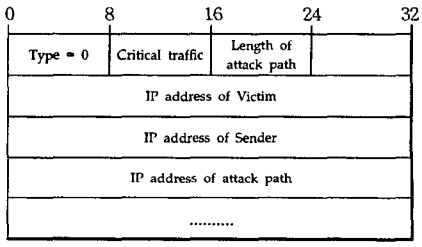
2. 프로토콜의 정의

본 프로토콜의 목적은, 피해자가 과다 트래픽의 수신을 탐지한 경우 그 과다 트래픽의 발신지를 역추적으로 탐색하여 공격자의 위치를 파악하고, 나아가 공격을 중지시키는 것이다. 과다 트래픽의 출처 및 트래픽 양의 측정을 위한 방법으로는 단순 망 관리 프로토콜(SNMP)을 통한 트래픽 측정을 사용하였다[2].

그 역추적은 내부적으로 정의한 메시지의 교환과 그 해석을 라우터들이 반복함으로서 수행된다. 공격자의 위치를 역추적하기 위해서는, 공격자와 피해자의 중도에 위치하고 있는 라우터들이, 각자 자신이 공격자로부터 과다한 트래픽을 전달받은 이웃하는 라우터를 파악해야 한다. 그러한 파악이 성공적으로 이루어지게 되면 역추적에 성공할 수 있으며, 최종적으로 공격자의 위치를 확인하게 되면 트래픽의 차단을 효과적으로 할 수 있게 된다.

프로토콜의 동작을 위해 교환해야 할 메시지의 종류는 다음과 같다.

① 서스피션 메세지(Suspicion Message) : 서스피션 메세지는 공격자로 의심이 가는 라우터에게 보내는 메시지이며, 패켓 필드는 다음과 같다.



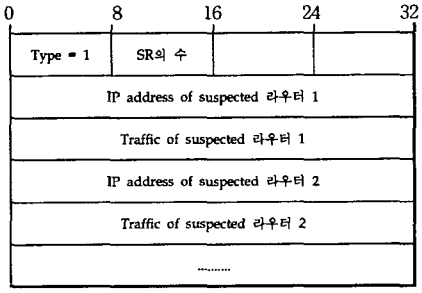
■ IP address of victim: 피해자의 인터넷 프로토콜 주소

■ IP address of sender : 현재 이 서스피션 메시지를 보내는 라우터의 인터넷 프로토콜 주소

■ Critical traffic : 정상적 트래픽의 한도를 의미한다. 트래픽이 이 한도를 초과하면 그 트래픽은 과다한 것으로 판단된다.

■ Attack path(optional) : 피해자와 공격자 사이의 라우터들의 인터넷 프로토콜 주소. 피해자와 공격자 사이의 중간 경로에 있는 라우터들이 하나씩 파악될 때마다 하나씩 엔트리가 추가된다.

② 설명 메세지(Elucidation Message) : 설명 메세지는 공격자로 간주되어 서스피션 메세지를 받은 라우터가, 자신은 공격자가 아님을 증명하기 위해 보내는 메시지로서, 설명 메세지의 패킷 필드는 다음과 같다.

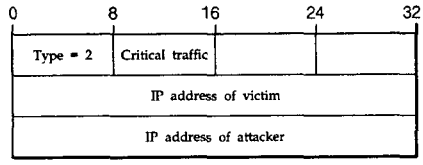


■ Self IP address : 자기 자신의 인터넷 프로토콜 주소

■ Suspected router의 수 : 의심되는 라우터의 개수

■ IP address of suspected router : 자신과 인접 라우터들 중에서, 임계 양 이상의 트래픽을 자신에게 발송시켜주는 라우터들의 인터넷 프로토콜 주소

③ 명령 메세지(Order Message) : 공격자의 위치가 파악되었을 때, 트래픽을 중단시키거나 감소시킬 것을 지시하는 내용을 전달하는 메시지로서, 명령 메세지의 패킷 필드는 다음과 같다.



■ IP address of victim : 현재 공격당하고 있는 라우터의 인터넷 프로토콜 주소

■ Critical traffic : 정상적 트래픽의 한도

■ IP address of attacker : 공격자의 인터넷 프로토콜 주소로서, 공격자 외에 패킷을 차단해야 할 대상을 별도로 지정해야 할 경우에도 이용될 수 있다.

또한, 라우터의 종류는 다음과 같이 정의된다.

① 공격자(Attacker)

한 호스트가 서비스 거부 공격을 수행하고 있을 때, 이 호스트가 연결되어 있는 라우터를 공격자라고 부른다.

② 피해자(Victim)

서비스 거부 공격을 당하는 호스트가 연결된 라우터를 피해자라고 부른다.

③ 공격 경로(Attack path)

공격자와 피해자를 포함하여, 그 가운데 있는 모든 공격 경로 상에 존재하는 라우터들의 연결을 공격 경로라 부른다.

④ 서스펙티드 라우터(Suspected Router)

공격 경로 상에 있는 라우터로서, 악의 여부와는 무관하게, 과다 트래픽을 보내고 있는 라우터를 서스펙티드 라우터라 부른다.

부가적으로 다음과 같은 분류도 정의한다.

⑤ 악의적인 라우터(Guilty Router)

악의를 가지고 공격에 적극적으로 임하는 라우터를 말한다.

⑥ 불확실한 라우터(Uncertainty Router)

현 시점에서 악의를 가졌는지 여부가 파악되지 않은 라우터를 말한다.

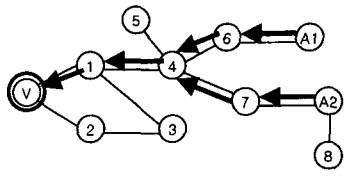
⑦ 결백한 라우터(Innocent Router)

나름대로의 절차를 거쳐, 악의가 없음을 확실하게 알 수 있는 라우터를 말한다.

3. 프로토콜의 동작

프로토콜은 피해자가 과다 트래픽을 받고 있는 것을 탐지한 경우나, 서스펙티드 라우터가 서스피션 메세지을 수신한 경우에 동작을 시작한다.

다음과 같은 네트워크를 가정하였을 때, 프로토콜의 동작은 V 피해자의 공격 감지로부터 시작된다.



공격당하고 있는 피해자는, 자신의 이웃하는 라우터 중에서 서스펙티드 라우터를 파악한다. 현재 피해자의 입장에서는 서스펙티드 라우터는 라우터 1밖에 없다. 따라서 라우터1을 서스펙티드 라우터로 간주하고, 서스피션

메세지를 발송한다. 피해자에게 서스피션 메세지를 수신한 라우터1은 공격 경로에 자신을 추가시킨 후, 마찬가지로 현재 자신이 인접해 있는 이웃하는 라우터들 중, 자신의 서스펙티드 라우터들에게 서스피션 메세지를 발송하는 동시에, 방금 자신에게 서스피션 메세지를 보낸 라우터 피해자에게 설명 메세지를 발송한다. 라우터1이 보낸 이 설명 메세지에는, 자신에게 과다 트래픽을 보내는 라우터4의 인터넷 프로토콜 주소와 그 트래픽 양이 기재되어 있어야 한다. 라우터1의 설명 메세지를 수신한 피해자는, 그 설명 메세지의 진위를 확인하기 위해 단순 망 관리 프로토콜을 이용하여 라우터4의 트래픽을 측정한다. 그 측정 결과, 라우터1이 주장하는 라우터4의 트래픽과 실제 라우터 4의 트래픽이 일정범위 이상 유사하다면, 라우터 1의 설명 메세지에는 이상이 없는 것으로 판별하여, 최종적으로 라우터1은 결백한 라우터라고 결론을 내릴 수 있다.

또한, 이 단순 망 관리 프로토콜(SNMP)측정에는 두 가지 조건이 있다.

조건1) 패켓의 다음 목적지는, 라우터1이어야 한다.

조건2) 수명(TTL)은 2로 제한하거나, 되돌아온 응답의 수명은 기본 값보다 2이상 감소되지 않은 상태로서, 라우터 1을 경유해서 도달하여야만 한다.

이것은 곧, 설명 메세지를 송신하는 라우터는, 자신의 바로 이웃한 라우터만을 의심되는 라우터로 주장할 수 있음을 의미한다. 또한 응답 패켓이 라우터 1을 경유하였는지 여부는 IP 프로토콜에서 옵션으로 제공하는 기능인 레코드 라우터를 이용함으로서 파악할 수 있다. [3]

프로토콜이 계속 진행되면, 라우터 6과 라우터 7은, 라우터 4에게 설명 메세지을 발송함과 동시에, A1, A2에게 서스피션 메세지을 발송한다.

공격자인 A1과 A2는, 서스피션 메세지을 수신하였을 때 취할 수 있는 방법이 세 가지로 요약된다.

1) 아무런 설명 메세지를 보내지 않는 경우
2) 정직한 설명 메세지를 보내는 경우
3) 허위 설명 메세지를 보내는 경우

공격자는, 이 세 가지 가운데 어떠한 행동을 취하더라도 적발을 피할 수 없다.

• 첫 번째로, 아무런 설명 메세지를 보내지 않는 경우에선, 서스피션 메세지를 발송한 측에서 일정한 타임아웃을 설정한 후, 그 타임아웃이 경과할 때까지 설명 메세지가 도착하지 않게 되면, 응답 없는 라우터를 공격자로 간주하게 된다.

• 두 번째로, 만약 서스피션 메세지를 수신한 공격자가 그의 정직한 설명 메세지를 보내는 경우에는, 그 설명 메세지의 서스펙티드 라우터의 넘버 필드에는 0이 적혀 있게 된다. 이러한 설명 메세지의 발송자는 공격자임을 파악할 수 있게 된다.

• 세 번째로, 공격자가 설명 메세지를 변조해서 보내는 경우를 생각할 수 있다. 이 경우에는, 단순 망 관리 프로토콜(SNMP)을 이용한 설명 메세지의 진위 확인과정을 거쳐서 이 라우터의 공격자 여부를 파악하게 된다. 지금의 예에서 공격자인 A1과 A2가 적발된 경우, 그들은 설명 메세지를 각각 라우터 6과 라우터 7에게 전달해야 한다. A1과 A2가 설명 메세지의 내용을 변조하는 방법과 그에 대한 대처 방법에는 다음과 같은 것이 있다.

i) 자신의 이웃하는 라우터로서 존재하지 않는 라우터를 자신의 서스펙티드 라우터라고 주장하는 방법 :

이 경우에는, 공격자가 주장하는 그의 서스펙티드 라우터에게 SNMP를 통한 GetRequest를 보내었을 때, 정상적인 GetResponse를 기대할 수 없게 된다.

ii) 자신의 이웃하는 라우터를 서스펙티드 라우터라고 주장하며, 허위 트래픽 양을 기재하는 방법 :

설명 메시지에 기재된 서스펙티드 라우터에 GetRequest를 보내 실제 트래픽을 파악한 결과, 돌아온 응답이 설명 메세지에 기재되어있는 트래픽과 차이가 있으면, 그 설명 메세지를 허위 설명 메세지로 간주할 수 있다.

iii) 자신의 이웃하는 라우터를 서스펙티드 라우터라고 주장하며, 실제 그 라우터의 옳은 트래픽 양을 기재하는 방법 :

공격자가 이러한 설명 메세지를 발송했다면, 이 설명 메세지에 명시되어 있는 모든 서스펙티드 라우터는 임계 트래픽 미만의 트래픽 양을 기재하고 있을 것이다. 따라서, 마치 정직한 설명 메세지를 발송했을 때와 마찬가지로, 이러한 설명 메세지를 발송한 라우터는 공격자임을 확신할 수 있게 된다.

이러한 과정을 통하여 라우터 6과 라우터 7이 공격자임을 파악하게 되면, 그들은 A1과 A2에게 명령 메세지를 발송한다.

명령 메세지를 수신한 공격자는, 명령 메세지의 공격자의 인터넷 프로토콜 주소필드를 파악한다. 그 필드의 값과 자신의 인터넷 프로토콜 주소가 일치한다면, 자신이 공격자인 경우이므로, 과다한 트래픽을 발송하고 있는 호스트를 차단하거나, 피해자를 목적지로 하는 패켓의 발송을 임계 트래픽 이하로 감소시킨다. 만약 호스트가 그 통지에도 불구하고 트래픽을 감소시키지 않으면, 피해자를 향한 그 호스트의 패켓 발송을 차단한다. 명령 메세지발송 이후에도 공격자의 트래픽 발송량이 감소되

지 않음이 감지되면, 피해자로부터 서스피션 메세지를 받았던 공격 경로상에 있는 라우터들은 공격자로부터 전송되는 패켓들 가운데 피해자를 목적지로 하는 패켓의 송출을 감소시킨다.

4. 성능평가

이 실험은 리눅스 환경에서 네트워크 시뮬레이터를 이용하여 수행되었다[4]. 본 실험에서는, 프로토콜의 정의에 따라 제작된 소스코드를 작성한 후, 공격자와 피해자를 지정하고, 공격자의 공격 경로 및, 공격자가 제시하는 허위 설명 메세지의 내용 등을 사용자가 명세 할 수 있도록 하였다. 실험 배경은 미주지역 내 기간망을 대표하는 게이트웨이의 네트워크를 대상으로 하였다[6].
실험에서의 가정 및 결과는 다음과 같다.

<실험 1> 공격자가 하나이며, 피해자가 하나인 경우

이상 없이 적발이 수행되었으며, 공격자가 멀리 있을수록 적발에 긴 시간을 소모한다.

Victim	Los Angeles
Attacker	Peterborough, Ottawa, Montreal 중하나

Node	적발에 필요한 시간 (sec)
Peterborough	8.500032
Ottawa	8.840066
Montreal	9.060079

<실험 2> 공격자가 공격경로를 변경하며 공격하는 경우

동일한 공격자가 동일한 피해자에게, 공격 경로만을 변경하여 재차 공격시도를 해 본 결과, 경로의 길이와 링크의 사정에 따라 적발 시간의 차이는 보였으나 공격 경로에 무관하게 전원 적발이 가능함을 확인할 수 있었다. 공격 경로가 길수록 평균적인 적발시간이 많이 소모되었다.

<실험 3> 공격자가 여러 개인 경우

6개의 공격자가 동시에 피해자를 공격하며, 피해자는 동시에 각자의 공격 경로로 서스피션 메세지를 발송하기 시작한다. 실험 결과는 다음과 같다.

Victim	Dallas
Attacker	Seattle, Tampa, Chicago, San Antonio, Hawaii, Salt Lake City

Node	적발에 필요한 시간 (sec)
Seattle	4.630007
Chicago	4.810001
Tampa	5.450005
San Antonio	12.280009
Hawaii	13.630016
Salt Lake City	14.230003

여기서, 각 공격자가 정직한 설명 메세지를 발송한 경우 적발에 필요한 시간은 다음과 같이 감소한다.

Node	적발에 필요한 시간 (sec)
San Antonio	0.400002
Chicago	1.310001
Tampa	2.090004
Salt Lake City	2.810000
Seattle	4.130001
Hawaii	5.010012

5. 결론 및 향후 연구 과제

본 연구에서 소개한 프로토콜은 서비스 거부 공격을 차단하기 위한 메커니즘을 제공한다. 또한 공격자가 다양한 경로를 통해 공격하면 할수록 공격 차단 망 역시 그 경로에 따라 새로 구축되므로, 심한 경우에는 공격자가 고립되는 경우도 발생된다.

이 논문에서 공격자로 동작하는 호스트 및 그 호스트가 속한 네트워크의 라우터들은, 실제 분산 서비스 거부 공격(DDoS)에 있어서는 실제 공격자보다는 공격 데몬인 경우가 대부분이다. 따라서 이 프로토콜로 인해 공격자로 지목 당한 호스트는 자신에게 트리노와 같은 분산 서비스 거부 공격용 소프트웨어가 설치되어 있는지의 여부를 파악해 보아야 할 것이다.

또한, 이 메시지들의 악용을 방지할 수 있는 로직이 보완될 것이 요구된다. 임계 트래픽을 매우 낮은 값으로 지정한 명령 메세지를 임의의 라우터가 보낼 수 있다면, 도리어 네트워크를 무질서하게 만들 수 있다. 따라서 공격자와 피해자사이의 핸드셰이킹에선 서로를 확인할 수 있는 상호인증이 보완되어야 한다.

또한, 서비스 거부 외 다른 종류의 공격에서도, 그 공격을 감지하는 방법이 고안하여, 서비스 거부 외의 다른 공격에 대한 본 메커니즘의 응용이 요구된다.

참고문헌

[1] Felix Lau, Stuart H. Rubin, Michael H. Smith, and Ljiljana Trajkovic, Disrtibuted Denial of Service Attacks

[2] 김현숙, 이명용, 전종명. 인터넷 트래픽의 측정동향 및 분석기법 연구. 정보통신연구 제14권 제1호. 2000.

[3] Behrouz A.Forouzan TCP/IP Protocol Suite. McGrawHill. 2000

[4] Jae Chung, Mark Claypool. NS by Example

[5] Kevin Fall, Kannan Varadhan. The NS Manual. UC Berkeley. 2001

[6] http://www.uu.net