네트워크 패킷 기반 DDoS 공격 탐지 시스템 설계

이원호, 한군희*, 서정택**
대천대학, 천안대학교*, 국가보안기술연구소**
e-mail: wheel@dcc.ac.kr, hankh@cheonan.ac.kr, seojt@etri.re.kr

Design of DDoS attack detection system based network packet

Won-Ho Lee, Kun-Hee Han*, Jung-Taek Seo**
Daecheon College, Cheonan University*, National Security Research Institute**

요약

본 논문에서는 최근의 가장 대표적인 해킹 방법인 DDoS 공격도구들을 분석하고, DDoS 공격에 대한 기존에 제시된 대응방안들을 검토하여 보다 적절한 대응을 할 수 있는 DDoS 공격 탐지 및 대응 시스템을 설계한다. 제안된 시스템은 탐지 모듈에서 탐지된 공격에 대해 관리자에게 보고하여 적절한 대응을 하고 침입으로 판정되는 패킷들에 대해서는 필터링을 실시하여 네트워크 레벨에서 필터링하고 차단할 수 있는 장점을 살릴 수 있다.

1. 서론

인터넷의 눈부신 발전을 통해 대용량의 데이터를 고속 전송할 수 있게 됨에 따라 개인 및 기업의 업무 효율을 향상시키고 생활의 질을 높여주며 국가 경쟁력을 강화시켜주는 긍정적인 효과를 거두고 있다. 그러나, 인터넷 사용자의 급속한 증가와 규모의 확대로 인해 외부인의 시스템 불법 침입, 중요 정보의 유출 및 변경·훼손·불법적인 사용, 컴퓨터 바이러스 및 서비스 거부 등과 같은 역기능들이 날로 증대되어 피해 규모가 심각한 수준에 이르고 있다.

몇 년 전, 야후 사이트가 해킹으로 인해 수 시간 동안 서비스가 중단되는 사태가 발생한 적이 있었다. 당시, 야후에 대한 해킹 분석과 대응책을 내놓기도 전에 이베이, 아마존, CNN, 증권거래소 등이 같은 해커들의 소행으로 보이는 동일한 수법으로 해킹을 당하여 한꺼번에 서비스가 중단되는 사태가 발생하였다. 이 해킹에 사용된 공격법은 분산 서비스 거부공격(Distributed Denial of Service Attack)으로 한 사람의 해커가 여러 서버를 해킹 한 후 공격용 프로그램을 데몬으로 설치하고 해커는 원격조정으로 목표 서버를 동시에 공격하도록 지시하는 방법이다. 국내에서도 같은 DDoS 공격 기법으로 인하여 국가 정보통신망의 대표 기관이라 할 수 있는 정보통신부 홈페이지가 몇 시간동안 서비스를 중단하는 사태가 발생하기도 하였다. 이렇듯 DDoS 공격은 대표적인 해킹 방법으로 아직까지 마땅한 대비책이 없다.

따라서, 본 논문에서는 분산환경에서의 DDoS 공격 도구인 TrinOO, TFN 등의 침입패턴을 분석하여 제안하는 DDoS 공격 탐지 및 대응 시스템의 설계에 적용하고 침입으로 판정되는 패킷들에 대하여 라우터나 방화벽에서 필터링을 실시하여 네트워크 레벨에서 필터링하고 차단할 수 있는 장점을 살릴 수 있도록 하였다.

2. 분산서비스거부공격(DDoS)

서비스거부공격은 일반적으로 공격자의 컴퓨터로부터 표적시스템과 그 시스템이 속한 네트워크에 과다한 데이터를 보냄으로써 시스템과 네트워크의 성능을 급격히 저하시켜 시스템에서 제공하는 서비스들을 인터넷 사용자들이 이용하지 못하도록 하는 기법이다. 서비스 거부 공격의 특징은 시스템 가용성에 대한 공격으로써 대상시스템의 권한을 획득하지 않고도 쉽게 공격이 가능하며, 공격자를 추적하기가 매우 어렵다. 또한, 공격대상시스템이 웹 서버와 같이 불특정 다수에 서비스를 수행하는 시스템인 경우 공격을 차단하기도 매우 어려운 실정이며, 공격방법이 쉬운 반면 피해는 상대적으로 크기 때문에 이에 대한 철저한 분석과 대응방안이 필요하다.

DDoS 공격은 많은 수의 호스트들에 패킷을 범람시킬 수 있는 DDoS 공격용 프로그램들이 분산 설치되어 이들이 서로 통합된 형태로 어느 목표시스템에 대하여 일제히 데이터 패킷을 범람시켜서 그 표

적시스템의 성능저하 및 시스템 마비를 일으키는 기법이다. DDoS 공격의 공격자는 하나 이상의 마스터를 제어할 수 있고, 각각의 마스터는 많은 데몬을 제어할 수 있다. 이 데몬에 의해서 표적 서버에 공격이 가해지게 된다. 서비스 거부 공격의 실제적인 형태는 TCP SYN flooding 공격, UDP flooding 공격, ICMP echo requesting 공격, ICMP broadcasting 공격(Smurf 공격) 등의 형태로 나타나며, 이러한 공격을 수행하기 위해서 다양한 공격용 도구들이 제작되고 있다. 분산 서비스 거부 공격용 도구들로 TrinOO, TFN 등과 같은 유닉스 계열의 공격 도구들이 사용되었으나, 최근에는 윈도우 계열의 W32/TrinOO 등이 출현하고 있다.

3. DDoS 공격에 대한 기존의 대응방안

DDoS 공격에 대응하기 위해서는 우선적으로 공격을 검출할 수 있는 방안이 필요하다. DDoS 공격 도구를 검출하기 위한 네트워크 모니터링 방법으로는 DDoS 분석용 네트워크 감시 도구인 스니퍼를 이용하여 마스터와 에이전트 사이에 오가는 ICMP 패킷을 검출하는 방법과 일부 유닉스 시스템의 경우에는 tcpdump와 같은 기능을 사용하는 ngrep이라는 유틸리티를 지원하여 ICMP 패킷을 검출하는 방법이 있다.

에이전트 데몬이 실제로 표적시스템(네트워크)에 DDoS 공격을 실행할 경우에는 표적시스템 쪽으로 에이전트의 IP를 추적하지 못하도록 발신지 주소를 위장한 데이터로 공격을 함이 보통이다. 그런데 어떤 네트워크의 라우터에서는 발신지 주소가 위장된 패킷은 바깥으로 나가지 못하도록 설정하는 경우가 있다.

마스터-에이전트간 ICMP 패킷 통신을 검출해 내기 위한 일반적인 방법으로는 마스터 시스템의 핸들러와 에이전트 시스템의 데몬은 서로 어떤 특정한 통신을 하기 위하여 암호화되지 않은 상태의 ICMP 패킷을 주고받는다. 따라서 tcpdump나 tcpshow 같은 네트워크 모니터링 도구를 이용하여 마스터-에이전트간 통신을 감시하여 마스터 핸들러나 에이전트 데몬 프로그램이 깔려있는 시스템을 찾을 수 있다.

마스터나 에이전트로 이용당하지 않기 위한 사실상 유일한 방법은 해킹 당하지 않는 것뿐이다. 또한 해킹 당하더라도 주기적인 점검과 모니터링을 통하여 침입자가 심어놓은 불법적인 프로그램들을 제거하는 것만이 유일한 대책이다. 또, 네트워크 스캐닝 도구나 모니터링 도구를 이용하여 자신의 네트워크 내에 공격 핸들러나 데몬이 깔려져 있는지 탐지 할 수 있다.

DDoS 공격에 대한 대응방안으로는 라우터의 외부 인터넷으로부터 들어오는 패킷을 필터링하는 방법과 Cisco 라우터의 Unicast RPF를 이용한 차단하는 방법, 라우터에서 RFC 1918에서 지정한 IP에서 들어오는 패킷을 모두 차단하는 방법 등이 있다.

4. DDoS 공격 탐지 및 대응 시스템 설계

DDoS 공격도구들을 분석하여 공격 특성 및 패턴을 도출하여 이를 규칙 집합을 이용한 탐지 모듈의 침입 패턴으로 이용하며, DDoS 공격 발생시의 네트워크의 특성들을 분석하여 Packet counting 탐지 모듈에 활용한다. 이와 같이 본 시스템은 두 가지 탐지 모듈을 장착한다. 규칙 집합을 이용한 탐지모듈은 기존 침입탐지시스템에서의 탐지 기법과 같은 방법으로 마스터-에이전트간의 통신상의 특성들을 검출하고, 공격 발생시의 특성을 패턴화하여 규칙집합으로 저장하고 있다가 들어오는 패킷들에 대하여 패턴매칭을 통한 DDoS 공격을 탐지한다. 이 탐지 모듈은 독립된 형태로 호스트에 에이전트로 심을 수 있어 호스트 기반 침입탐지시스템으로 활용이 가능하게 설계하였다. 또한, 규칙집합을 이용한 탐지 모듈은 공격자가 공격형태를 조금씩만 변화를 주어도 그 공격 패턴이 규칙 집합에 정의가 되어있지 않으면 탐지가 불가능해 지는 특성을 지닌다. 반면, 계속해서 규칙 집합을 추가시킴으로써 변화하는 공격 특성에 능동적으로 대처할 수 있다는 장점이 될 수도 있다. 본 시스템에서는 일반적인 네트워크 레벨의 탐지 방법으로 Packet counting을 이용한 탐지 모듈을 별도로 설계하여 장착하였다. 이로써 공격에 대한 탐지율을 극대화 할 수 있고, 이 탐지 모듈들은 서로 독립적으로 활용이 가능하다.

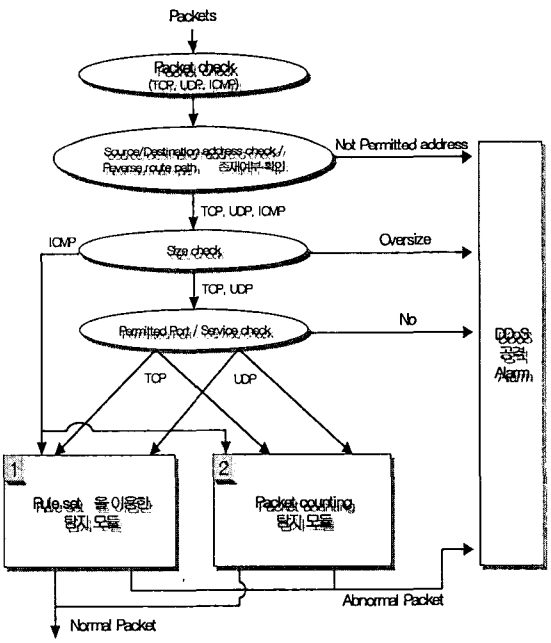
DDoS 공격탐지시스템에 의해서 탐지된 공격에 대해서는 관리자에게 보고를 하거나 방화벽과 라우터에 보고하여 적절한 대응을 하게 된다. 관리자는 내부 시스템이 공격의 중간 단계인 마스터나 에이전트로 사용되고 있는 것이 발견되면 설치된 공격도구를 찾아 제거하며, 마스터로 발견된 시스템의 경우에는 IP 리스트 파일을 찾아 그 사이트들에 접속하여 침입의 흔적이 있는지 확인할 수 있다. 또한, 얻어진 리스트를 이용해서 모든 DDoS 공격 데몬을 멈추게 할 수 있다. 방화벽과 라우터는 공격으로 탐지된 패킷의 발신지 IP 주소와 관련 정보를 보고 받아 공격으로 들어오는 패킷들에 대해서 필터링을 한다.

DDoS 공격탐지시스템 내부의 규칙 집합을 이용한 탐지 모듈 설계를 위해 우선적으로 공격에 사용되고 있는 공격도구인 TrinOO, TFN 등의 특성, 즉

공격도구들의 공격 시나리오, 사용하는 통신포트, 암호화 전송 및 패스워드, 마스터와 에이전트간에 통신상에 주고받는 메시지 등을 분석하여 이 특성들로부터 패턴 매칭에 사용할 패턴들을 규칙 집합으로 저장할 수 있다.

평상시의 네트워크 트래픽 양을 조사하고, 일반적인 DDoS 공격 시 유입되는 시간당 패킷의 양을 설정하는데 활용할 수 있는 정보를 만들어야 한다. 이는 Packet counting을 이용한 탐지 모듈에서 공격을 탐지하는데 사용된다. TCP, UDP, ICMP 패킷 모두를 공격 탐지 대상으로 한다.

DDoS 공격 탐지 알고리즘은 Packet check 모듈에서는 우선 네트워크에 들어오는 패킷들에 대하여 DDoS 공격에 사용되는 프로토콜인 TCP, UDP, ICMP 프로토콜에 대해서만 필터링 대상으로 한다. 이렇게 함으로써 방대한 프로토콜에 대하여 DDoS 공격과 관련된 프로토콜 패킷만 선별하여 공격 탐지 대상으로 패킷의 규모를 축소할 수 있다.



Source/Destination address check 모듈은 사전에 취득한 보안정보로부터 공격의 빈도가 높은 네트워크 혹은 호스트로부터의 접근을 탐지하여 주소 필터링을 수행하고, 네트워크 주소가 신뢰할 수 있는 DNS에 등록되지 않은 주소를 탐지하며. 발신지 주소가 내부 주소를 가지고 들어오는 패킷은 IP 스푸핑된 패킷으로 판별한다. Reverse route path 존재 여부 확인은 Cisco 라우터에서 사용하는 방식으로 패킷이 들어올 때 패킷의 입력 인터페이스로의 reverse path route가 존재하는지를 확인한다. 만일 발신지 IP 주소가 위장된 것이라면 발신지 IP로부터 라우터에 들어오는 입력 인터페이스로의 reverse path route가 존재하지 않을 것이다. 그러므로, reverse path route가 존재하는 패킷만을 통과시킨다.

Size check 모듈은 Oversize를 이용한 DDoS 공격을 탐지하는 모듈로서, ICMP 패킷을 사용하는 ping을 이용한 조작된 크기의 패킷 전송 공격유형들을 탐지한다.

Permitted Port / Service check 모듈에서는TCP/UDP 프로토콜을 기반으로 하는 네트워크 패킷 중 이미 발표된 보안 문서들로부터 침입에 취약한 것으로 평가되어 네트워크 관리자로부터 사용이 허가되지 않은 네트워크 접근을 시도하는 서비스에 대하여 탐지한다. 특정 포트를 대상으로 이루어진다.

5. 결론

본 논문에서 제안하는 네트워크 패킷 기반 DDoS 공격 탐지 및 대응 시스템은 데이터 링크 계층으로부터 네트워크 계층의 정보들을 기반으로 각 탐지 기능별, 계층별로 모듈화 작업을 하였고, 내부적으로는 크게 규칙 집합을 이용한 탐지 모듈과 Packet counting을 이용한 탐지모듈로 설계하였다.

향후 연구에서는 기존의 네트워크 기반의 침입탐지시스템과의 통합과 공격에 대한 역추적 기능에 대한 연구가 필요하다. 또한, 방화벽 및 기타 통합적인 보안 시스템으로의 확장성 등을 추가하여 통합 보안 관제 시스템으로의 확장이 필요하다. 이러한 연구결과로부터 전체 네트워크 보안 관리체계에 있어 관리자에게 보다 강력한 네트워크 보안성을 제공할 수 있을 것이다.

참고문헌

[1] B.Mukherjee, T.L. Heberlein, and K.N.Kevitt, "Network intrusion Detection", IEEE Network, 8(3): 26-41, May/June 1994

[2] M.J. Ranum et al., "Implementing a generalized tool for network monitoring," Proc. 11th Systems Administration Conf. LISA'97, San Diego, CA, October 1997.

[3] 정현철 외, "분산 환경에서의 서비스 거부 공격 분석 보고서", 한국정보보호센터, 1999.12

[4] 임채호, "야후 등 유명 웹 사이트 해킹 사고와 분산서비스거부공격 대책", 정보보호21C, 2000.3