韓國 컴퓨터情報學會 論文誌
第10卷 第5號, 2005. 11.

2005-10-5-2-13

TCP/IP 공격에 대한 보안 방법 연구

박 대 우*, 서 정 만**

A Study of Security Method against Attack in TCP/IP

Dea-Woo Park*, Jeong-Man Seo**

요 약

오늘날 사이버세상에서 네트워크의 성능은 정당한 내용의 요청에 대한 증가에 의해서 뿐만 아니라 악의적인 활동의 증가에 의해서도 영향을 받고 있다. 이 논문에서 네트워크 성능에 영향을 주는 악의적인 해커의 TCP/IP를 이용한 DoS 공격 및 DDoS 공격, SYN Flooding을 이용한 공격, IP Spoofing 공격 등을 연구한다. 이 공격들에 대비하여 방어하는 네트워크 레벨과 게이트웨이 레벨 및 응용계층 레벨에서의 패킷 필터링 방법을 제안한다. 또한 웹 서버에서의 캐시 서버, 미러 서버와 CDN을 사용하여 콘텐츠를 분배하는 방법에 대해 제안한다. 이러한 제안들은 공격자의 공격에 대응하는 방법으로 유용하게 사용되어질 것이다.

Abstract

In today's cyberworld, network performance is affected not only by an increased demand for legitimate content request, but also by an increase in malicious activity. In this paper, we research that network performance was affected by an increase in malicious Hacker who make DoS Attack, DDoS Attack, SYN Flooding, IP Spoofing, etc. in using TCP/IP. We suggest that Packet filtering in Network Level, Gateway Level, Application Level against to protect by Hacker's attack. Also, we suggest that content distribution in Web Server approaches to mitigate Hacker's activity using Cache Sever, Mirror Sever, CDN. These suggests are going to use useful protection methode of Hacker's attack.

▸ Keyword : 패킷필터링(Packet Filtering), content distribution, DoS, Hacker Attack, TCP/IP.

• 제1저자 : 박대우
• 접수일 : 2005.10.14, 심사완료일 : 2005.11.07
* 숭실대학교 컴퓨터학과, ** 한국재활복지대학 컴퓨터게임개발과 교수

Ⅰ. 서 론

인터넷을 통한 업무의 증가와 더불어 네트워크에서의 트래픽(traffic)은 계속 증가하고 있다.

멀티미디어 데이터를 포함하는 인터넷 서비스의 증가는 (그림 1)과 같은 TCP/IP(Transmission Control Protocol /Internet Protocol)를 중심으로 하고 있다.

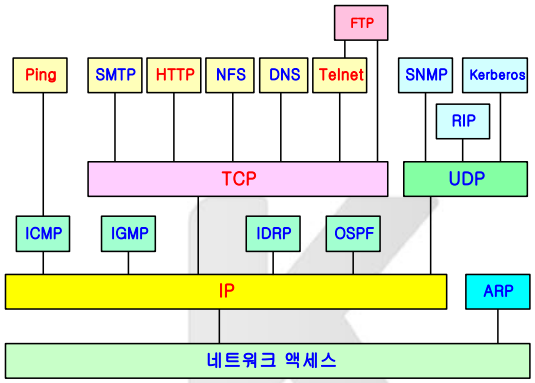

그림 1. TCP/IP 프로토콜
Fig. 1 TCP/IP Protocols

이때 인터넷 서비스를 위한 네트워크 성능에 영향을 미치는 중요한 문제 중의 하나는, 순간적으로 리소스의 과부하 상태가 만드는 네트워크 통신량의 폭주이다.

네트워크 통신량의 폭주가 인터넷 업무의 증가에서 비롯된 것과는 달리, 악의적인 활동에 의해서도 통신량의 폭주가 될 수 있다. 즉 인터넷 업무를 방해하기 위해 불법적인 행동으로 네트워크에 대한 폭주를 일으키는 활동을 한다.

본 논문에서는 인터넷 서비스를 하기위한 프로토콜인 TCP/IP의 취약성을 이용하여 네트워크 사용을 방해하는 TCP/IP를 이용하는 여러 가지의 공격에 대하여 연구하고, 이들의 공격에 대응하는 보안 방법들을 연구하기로 한다.

공격의 대응 방법으로 사용되는 시스템 보안과 네트워크 보안 방법에서 가장 일반적인 패킷 필터링의 방안들을 제안한다. 또한 요즘 사회에서 이슈화되고 있는 인터넷 웹 서버의 다운으로 발생하는 문제를 인식하여 네트워크 트래픽을 줄이고 인터넷 콘텐츠의 내용 분산 접근 방법들을 제안하여 정보 보안에 도움이 되는 방법들을 연구한다.

Ⅱ. 관련연구

2.1. TCP/IP의 취약성

(그림 2)는 서버와 클라이언트 사이에서 TCP의 3단계 (Three way handshake) 연결설정과 해제의 과정을 보여준다.

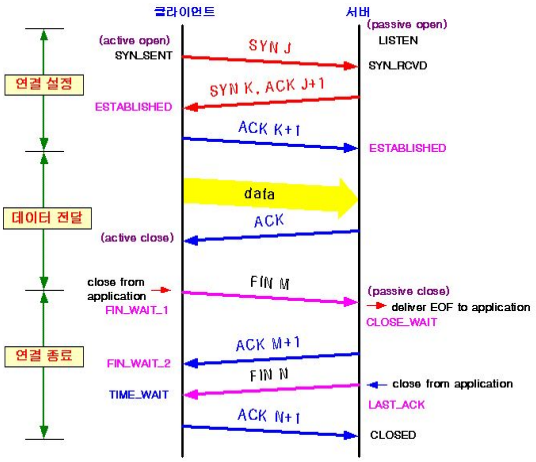

그림 2. TCP 3핸드 쉐이크 연결 설정 과 해제
Fig. 2 3 hand shake of TCP connecting and disconnecting

연결 설정은 클라이언트가 SYN J 세그먼트를 보내 서버에 연결 설정을 한다. 이 요청에 대한 응답으로 SYN K 세그먼트를 보낸다. 클라이언트가 서버에 대한 확인응답인 ACK K+1 을 보낸다. 연결 해제는 데이터의 송수신 후에 서버에 FIN M세그먼트를 보내 연결 해제를 요청하면 클라이언트가 확인응답을 보내 연결 해제를 알린다. 서버가 클라이언트에 FIN N 세그먼트를 보내 연결 해제를 요청하면, 서버가 이에 대한 확인응답을 보낸 연결 해제를 알린다.

이때 서버와 클라이언트 사이에 SYN 와 ACK의 연결 설정 중에는 대기 상태(half open)가 되어 상대편이 응답하지 않으면 접속확립(full connection)이 되지 않으며, 큐

(Queue)에서 접속내용이 제거 되지 않고 쌓이게 된다. 또한 TCP의 소켓(socket)에서 세그먼트를 동시에 처리하는 데에는 한계가 있다. 이 문제가 TCP의 취약성이다.

그림 3. IP 데이터그램의 헤더
Fig. 3 head of IP datagram

또한 TCP/IP는 프로토콜이 설계될 때, 데이터그램 자체가 전혀 암호화 되지 않고 전송되므로, 네트워크 상에서 (그림 3)과 같은 구조를 가진 IP 패킷을 가로채서(sniffing) 순서에 맞게 재조합하면, IP의 근원지주소, 목적지주소 뿐만 아니라 서비스유형과 ID나 패스워드 까지도 알아 낼 수 있다. 이 문제 역시 IP의 취약성이다.

2.2. TCP/IP 공격

2.2.1 DoS(Denial of Service) 공격

침투자는 공격자 대상의 TCP 패킷을 가로채어 TCP의 패킷을 위조한다. 공격자는 위조된 TCP 패킷을 이용하여 공격대상 서버로 SYN을 요청한다. 이때 또 다른 TCP의 패킷을 위조하여 다른 여러 호스트들을 가장하여, 같은 공격대상 서버에게 SYN을 요청한다. 공격 서버가 처음 SYN에 대해 대기상태인 half open을 유지하고 있는 동안에 위조되어 처리되지 않는 다른 SYN가 백로그 큐(Backlog Queue)에 쌓이게 되면서, 더 이상의 연결서비스를 할 수 없는 서비스 거부 상태(Denial of Service)가 되어 해당 포트의 서비스는 중단된다.

DoS 공격자들의 초기 형태는 하나의 호스트가 하나의 다른 서버를 공격하는 형태이다. 전통적인 DoS 공격 모델에서는 공격자와 공격 목표인 웹 서버 공격과 같은 단순한 1:1 공격의 형태였다.

다음으로 출현한 공격의 모델은 종속 호스트(Slave Host)들을 이용하는 방법이다. 이 경우 공격자가 마치 지휘자(Manager)처럼 명령에 따라 목표를 공격할 준비가 되어 있는 종속 호스트들을 가지게 된다. 즉, 1:n의 공격 형태를 갖추게 되는 것이다.

최근의 공격자는 대리인(Agent)을 움직이는 배후조종자(Master)의 지위를 획득한다. 공격자는 타인의 시스템에 공격 명령을 암호화 하여 자기를 배후조종자로 하는 하위의 대리인들을 정하고 피라미드식의 침투 세력을 확보한다. (그림 4)처럼 공격자의 명령을 통해 대리인들을 조정하고 대리인들은 명령에 따라 종속 호스트들을 조정하여 목표가 되는 서버를 일순간에 공격하여 하여 서비스가 중지 되게 한다.

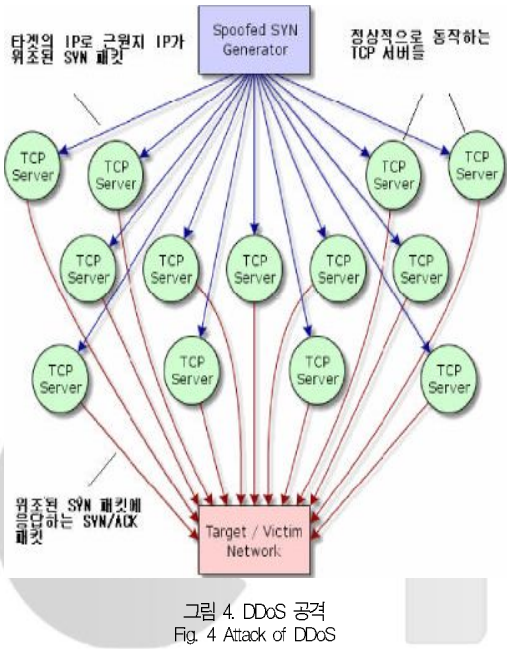

그림 4. DDoS 공격
Fig. 4 Attack of DDoS

이 모델의 원래 모델에서 분산된 형태이기 때문에 분산 서비스 거부공격인 DDoS(Distribute Denial of Service) 공격[1]과 DRDoS 공격[2] 이라고 부른다.

또한 DDoS 공격은 공격대상 서버로부터 접속 연결 SYN 요청에 대한 응답을 처리하지 않아, 공격하는 호스트들에게 오는 응답을 빗나가게 하여 종속 호스트의 서버가 네트워크 트래픽의 출발지인 것처럼 공격을 한다. 그리고 추적을 하여도 공격자가 노출되지 않는 n:n의 공격을 한다.

2.2.2 Buffer Overflow를 이용한 공격

C언어에 의해서 작동되는 유닉스 운영체제의 네트워크 연결설정 처리 과정에서 IP 패킷의 이름 등을 길게 하여 메모리 버퍼(memory buffer)를 차지하게 하여 공격 대상 네트워크 서버의 정상적인 작동을 방해하는 공격이다.

2.2.3 Smurfing을 이용한 공격

IP 기반의 핑(Ping)을 이용하여 출발지 주소를 속여서 ICMP_ECHO_REQUEST를 브로드캐스트 하게 하면 이를 수신한 모든 호스트(host)들이 출발지로 ICMP_ECHO_REPLY를 보내 전달하므로, 공격대상인 출발지 서버로 응답이 증가하여 네트워크 트래픽을 형성하여 서버의 기능을 마비시킨다.

2.2.4 Land Attack

공격대상 서버에 대한 출발지와 목적지가 동일한 IP 패킷을 위조하여 보내면, 수신한 호스트는 패킷의 출발지를 목적지로 변경하여 응답을 보내므로, 출발지인 서버는 자기 자신에게 패킷을 보면서 서버 자원의 과부하로 네트워크 트래픽으로 기능이 마비된다.

2.2.5 Flash-Crowds

공격자는 공격대상의 서버에 합법적인 트래픽을 발생시키도록 유도하여 일순간 동시에 TCP/IP 접속을 시도하는 것이다. 공격대상 서버는 예상하지 못한 정도의 트래픽에 직면하면 일반적으로 예상된 설계 용량으로는 트래픽 처리를 하지 못한다.

불법적인 DDoS공격 결과와 유사한 Flash-Crowds는 고의가 아니게 DoS 공격과 같은 문제를 일으키게 되어 다른 사용자의 접속을 거부된다.

2.2.6 SYN Flooding을 이용한 공격

침투자는 IP 패킷의 출발지 주소를 위조하여, 존재하지 않거나 도달할 수 없는 주소를 만든다. 공격자는 (그림 5)처럼 위조된 IP 패킷으로 공격대상 서버에 TCP 커넥션을 통해 연결요청을 하면서 대기 상태를 만들고, 위조된 패킷의 ACK의 전달이 안 되어 서버에서 접속확립이 안되게 된다.

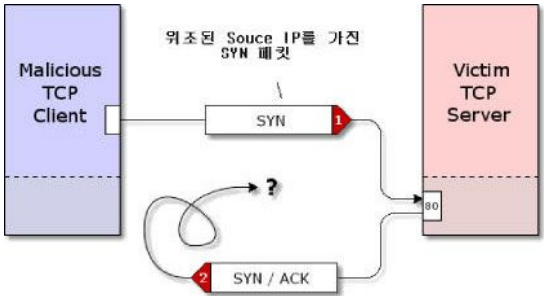

그림 5. TCP SYN를 이용한 공격
Fig. 5 Attack of TCP SYN

결국 공격대상 서버의 큐(queue)에서 접속 내용이 쌓이게 하여, 큐가 가득 차게 되면 정상적인 접속 요구를 못하게 되어 네트워크 서비스가 중지 되게 된다.

2.2.7 IP Fragment 공격

침투자는 IP 패킷의 단편화(Fragment)에 관련된 Offset 값에 대한 의도적인 변경을 통하여 네트워크에서의 MTU(Maximum Transmission Unit)를 초과하는 IP 패킷을 만든다. 공격자는 이 패킷을 공격 대상 서버에 보내어 네트워크 상의 대기 큐에서 재조립하거나 패킷의 적재를 일으키게 하여 네트워크의 흐름을 방해한다.

2.2.8 IP Spoofing 공격

침입자는 신뢰성이 있는 호스트의 주소를 포함하는 발신지 IP 주소 필드를 갖는 패킷을 만들고 TCP의 접속 절차에 따르는 SYN와 ACK의 일련번호를 샘플링하여 추측한다. 공격자는 신뢰성이 있는 이 호스트를 DoS공격 등으로 무력화 시킨다. 공격자는 정상적인 IP처럼 속이는 스푸핑(Spoofing)을 이용하여, 공격대상 서버에 TCP의 접속 절차에 따르는 SYN와 ACK의 일련번호를 사용하여 정상적인 접속을 한다.

공격자인 호스트는 공격대상 서버에 정상적인 접속인 것처럼 속여서 공격자가 원하는 정보를 취한 후에 대상을 공격한다.

2.2.9 Sniffering 공격

침투자는 네트워크에서 전송되는 패킷을 스니핑하고 이 패킷을 순서에 맞게 재조립하여 원래의 데이터를 추출한다. 이더넷(Ethernet)의 특성 중 하나인 패킷을 전달 시에 출발지와 목적지의 주소를 참조하여, 호스트는 본인의 주소만을 받아드리고 나머지는 폐기(drop)한다.

공격자는 Promiscuous mode를 통해 모든 패킷을 잡아들여서, 공격자가 원하는 ID와 Password 등의 정보를 해킹한 후 공격대상 서버를 공격한다.

2.2.10 Teardrop 공격

MTU값에 대한 패킷 조각의 크기가 크지 않는 것만을 검사하지만, 작은 것은 검사하지 않는다. 침투자는 IP 패킷의 단편화에 관련된 Offset 값을 의도적으로 음수 값이 되도록 조작한다.

공격자는 이 패킷의 헤더 값을 음수로 조작한 두개의 패킷조각을 이용한다. 이 공격의 결과로 패킷의 내용이 너무 많이 복사되어 버퍼를 가득 차게 하여 서버의 기능을 마비시킨다.

2.2.11 New Teardrop/Bonk/Boink 공격

위 2.2.10의 Teardrop공격과 유사하나 UDP 패킷을 구성하는 두 번째 조각의 Offset을 이전 패킷조각의 UDP 헤더 위치로 설정하여, 나중 패킷 조각의 내용이 이전의 헤더 내용을 덮어쓰게 함으로써 불안전한 패킷을 계속 생성 시키게 한다. 결국 공격자의 계속된 조작된 패킷의 전송으로 서버의 속도가 현저히 감소되거나 시스템의 중단을 초래한다.[3].

이 외에도 Windows의 서버 시스템의 불안전성을 이용한 TCP/IP 공격 등이 있다.

III. 패킷 필터링 방법

인터넷 서비스의 실행을 하는 것은 네트워크에서의 정보 전송을 수행하는 패킷이다. 패킷은 데이터를 저장하고 전달하기 위한 네트워크의 가장 작은 논리적 단위이다.

패킷은 네트워크에서 정보전달을 위한 헤더정보인 출발지 주소, 목적지 주소, 프로토콜과 목적지 포트 패킷의 길이, 우선순위, 에러의 수정 정보 등의 요소를 가진다.

따라서 네트워크의 다른 계층과 다른 네트워크를 통해서 출발지에서 목적지로 전달될 때, 선택적인 패킷 필터링 규칙을 설정하여 패킷의 통과 여부를 결정하여 접근제어를 하는 정보 보안에서 꼭 필요한 중요한 방법이다.

패킷 필터링 규칙은 네트워크 계층의 경계에서 세워지면서 접근제어를 통해 인터넷 서비스를 하는 패킷을 제어한다. 따라서 네트워크 트래픽의 불필요한 증가를 감소시키면서 위에서 언급된 TCP/IP의 취약성을 이용한 불법적인 해커의 공격으로부터 일차적인 안전성을 부여한다.

본 논문에서는 인터넷에서 패킷 필터링을 적용할 수 있는 레벨을 (그림 6)과 같이 네트워크 레벨에서 수행하는 라우터(Router)[4]와 게이트웨이(Gateway) 레벨에서 수행하는 방화벽(Firewall)[5], 그리고 응용(Application) 레벨에서 수행하는 프락시 서버(Proxy Server)로 나누어 패킷 필터링[6]의 기술을 제안한다.

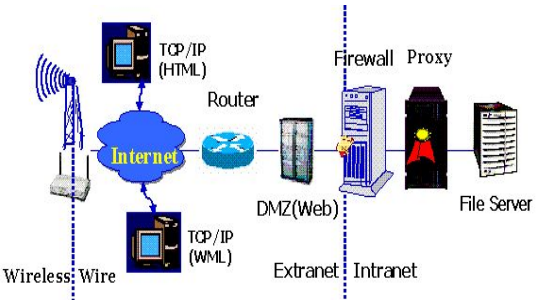

그림 6. 3 패킷필터링 레벨
Fig. 6 3 level of Packet Filtering

3.1 네트워크 레벨 패킷 필터링

(그림 6)에서 네트워크 레벨의 라우터에서 패킷 필터링은 인터넷 서비스에서 트래픽으로 인한 오버로드와 악의적인 해커로부터 정보보안을 할 수 있는 첫 번째 단계이다.

라우터는 패킷들의 방향을 바꾸어 출발지 호스트에서 목적지 호스트로 찾아가도록 하는 장치이다. 두 호스트 사이에서 라우터는 연속적으로 변하는 네트워크의 라우팅 테이블을 주기적으로 업데이트 하면서 동적인 활동을 하고 있다. 라우팅 테이블은 라우터의 정보와 특정 라우팅 프로토콜을 사용하는 것과 같은 방법으로 통신하면서 네트워크 트래픽을 분산시키면서 동작되어야 한다.

라우터에서의 패킷 필터링은 네트워크를 통해 증가시키는 잘못된 패킷의 정보를 차단 할 수 있다. 그리고 한 방향으로 패킷을 걸러내어 네트워크 시스템에서 불필요한 트래픽을 제어할 뿐만 아니라, 둘 이상의 라우터 프로토콜 사이에서 공유하는 정보에 의한 트래픽의 중복이 일어나는 것도 피할 수도 있다.

네트워크 레벨에서 문제는 정상적인 패킷으로 위조된 잘못된 정보를 갖는 패킷으로 트래픽을 야기 시키는 문제이다. 즉 라우터의 재 분산 방법은 잠재적으로 부정확한 라우터를 만들 수 있다. 어떤 경우에는, 라우팅 테이블의 루프 안에서 블랙홀 현상을 일으킬 수 있다. 또 다른 문제는 라우터의 피드백이다. 즉 재분배된 라우터를 통해 잘못된 방향으로 패킷의 방향을 통지해 주는 것이다.

공격자의 위조된 패킷 정보에 의해 부정확하게 업데이트 된 라우팅 테이블은 보안에 취약성을 나타낸다. 이 결과 네트워크 과부하를 크게 일으킬 수 있을 뿐만 아니라, 특별한 목표로 경로를 재설정을 하여 DoS 공격 상태를 야기 시킬 수도 있다.

3.2 게이트웨이 레벨 패킷 필터링

네트워크 레벨에서는 위조된 패킷 정보에 의해 부정확하게 업데이트된 라우팅 테이블은 보안에 취약성을 나타낼 뿐만 아니라, 허용된 시스템의 패킷들이 특별한 포트로의 접속을 통제하거나 허용하는 패킷 필터링 규칙을 사용할 수 없다.

따라서 (그림 6)과 같이 내부 시스템과 외부 네트워크 사이에 게이트웨이를 설정하고, 여기에 방화벽이나 스크린 라우터 등 정보보호 시스템을 설치한다. 즉 내부 네트워크를 의미하는 정보 시스템의 경계인 게이트웨이 레벨에서 정보 보안을 실시한다.

즉 외부 네트워크에서 내부 네트워크로 들어오는 모든 패킷들을 통과 시키거나, 허락 되어지지 않은 패킷들은 폐기하는 패킷 필터링을 실시한다. 패킷 필터링 과정은 정당한 주소를 가지고 내부 네트워크로 들어오는 모든 패킷의 헤더들은 벗겨서 조사하는 과정이다. IP 패킷의 헤더를 소스와 목적지 주소를 필터링[7] 하는 것은 본 논문에서 연구된 Flooding이나 Spoofing과 같은 문제를 피할 수 있게 한다. 즉 패킷을 브로드캐스트 하거나 멀티캐스트(multicast) 하는 네트워크 시스템은 특정한 주소를 사용하는 네트워크 시스템에서 목적지의 주소를 허용한다.

이러한 패킷들은 네트워크 레벨에서 트래픽을 야기 시킬 수 있다. 공격자는 이러한 방법들은 동원하여 공격대상 시스템에 트래픽을 야기 시켜 있다. 하지만 게이트웨이 레벨에서 패킷 필터링 규칙을 설정하여 목적지 주소를 브로드캐스트 하는 패킷을 폐기할 수 도 있다. 그리고 인증된 사용자에 의해서 들어오는 패킷만을 받아들이도록 접근제어를 통해 게이트웨이에서 패킷 필터링을 할 수 있다.

패킷 헤더의 필터링에서 특별히 사용되어지는 요소는 포트(Port) 번호이다. 각각의 TCP/IP에 연결된 서비스는 네트워크 시스템에 의해 연결된 포트 번호를 제공한다. 예를 들어 80번 포트는 웹 서비스, 23번 포트는 텔넷, 그리고 22번 포트는 SSH(Secure SHell) 서비스 포트이다. 이중 자료 유출 가능성이 높아 보안 취약성이 높은 텔넷 서비스는 점점 SSH로 대체되어지고 있다.

게이트웨이 레벨에서 패킷 필터링은 보안에 문제되는 서비스의 포트를 쉽게 막음으로써, 네트워크 레벨의 보안에 취약성이 있는 서비스의 보안문제를 해결하게 되었다.

3.3 응용 레벨 패킷 필터링

내부의 허용된 사용자가 시스템의 브로드캐스트 주소를 가진 패킷을 계속 보내는 경우에, 네트워크 레벨이나 게이트웨이 레벨에서의 필터링은 인증된 사용자에 의한 패킷이므로 내부 시스템에 트래픽을 야기 시켜, 네트워크에 오버로드를 걸리게 한다는 약점이 있다.

네트워크 레벨을 통한 패킷들이 내부 시스템과 외부 네트워크 사이에 게이트웨이 레벨을 지나간 후, (그림 6)과 같이 방화벽의 상위 레벨이나 내부 네트워크에 설치된 응용 레벨에서 프락시 서버의 패킷 필터링을 통해 인증 받지 않는 서비스[8]나 트래픽을 일으키는 요인을 내재하고 있는 패킷에 대한 필터링 규칙을 동적으로 적용할 수 있다.

TCP/IP 연결을 통해 내부 인터넷 서비스 호스트는 외부 호스트와 TCP 연결을 성립 할 것인지를 결정하는 것은 TCP 연결로 외부 호스트가 보내는 패킷에 의해 결정된다. 연결이 성립되어진 후의 패킷은 이미 네트워크나 게이트웨이에서 통과된 패킷이다.

하지만 본 논문에서 연구된 Sniffering 공격이나 New Teardrop/Bonk/Boink 공격을 행하는 패킷들은 TCP/IP을 응용하는 서비스를 수행하는 패킷들로 위장할 가능성이 있다. 즉 내부 네트워크에 도달하기 이전에 네트워크 레벨이나 게이트웨이 레벨에서의 패킷 필터링에서 빠뜨렸을지 모르기 때문에, 응용 레벨에서 프락시 서버를 통해 패킷 필터링을 한번 더 검사 할 수 있다. 또한 프락시 서버의 패킷 필터링은 사용자의 서비스 사용으로 인한 패킷을 허용하고, 이들 서비스는 내부 프락시에서 받아들여진 패킷들은 한번 더 검사하고 평가하여, 패킷에 대한 감사기록을 남길 수 있다.

가장 중요한 점은 만약 네트워크를 통해 들어오는 트래픽으로 인해 네트워크나 게이트웨이에서 인터넷 트래픽으로 인한 오버로드를 일으킨 경우 내부 서비스 서버들은 속수무책으로 다운 된다는 것이다. 따라서 내부 네트워크의 모든 리소스 자원을 보호하는 최후의 보루로써의 역할을 응용 레벨에서 프락시 서버가 수행하는 것이다.

다양한 서비스에 대해 인증을 받은 많은 사용자의 서비스에 대한 인증과 감사기록 및 부인방지를 위해서는, 내부의 프락시 서버를 이용한 필터링을 함으로써 접근제어와 서비스제어 및 인증과 부인방지 감사기록 보존과 같은 정보보안 정책을 수행할 수 있다.

Ⅳ. 콘텐츠 배분 방법

일반적으로 웹 서버를 설치할 때, 네트워크의 용량을 예측하고, 비용과 효율성과 보안성 및 예상 최대 접속자 수 그리고 네트워크 트래픽 등을 예측하여 네트워크의 시스템을 설계한다. 이러한 이유로 트래픽이 많고 콘텐츠가 홍보용으로 설치된 웹 서버는 내부 네트워크와 외부 네트워크 사이에 DMZ(Demilitarized Zone)를 설치하고 이 부분에 웹 서버를 설치하기도 한다. 웹 서버를 포함한 네트워크 자원의 부족한 리소스에 예측하지 않는 네트워크 트래픽이 갑자기 증가된다면, 접속 요청의 서비스의 여유가 없는 상태에서 서비스는 지연되고 결국은 네트워크 시스템은 트래픽으로 인하여 인터넷 웹 서비스가 중단된다.

TCP/IP의 취약점을 이용하는 공격자는 공격대상 웹 서버의 같은 콘텐츠를 요청하면서, 본 논문에서 연구한 DoS 공격 및 SYN Flooding 공격 등을 실시하여 네트워크 트래픽을 야기 시켜 공격 대상 시스템의 과부하를 발생시킨다.

이러한 공격에 대비하는 효율적인 방법 중에 하나가 요청받는 콘텐츠를 복사하여 웹 서버와 네트워크의 능력을 증가시키는 것이다. 웹 캐시(Web Cache)와 미러 서버(Mirror Server)는 과부하가 일어나는 동안 콘텐츠의 분배 조절자로서 웹 서버를 위하여 콘텐츠를 복제하여 저장하는 네트워크 서버 기술이다.

본 논문에서는 웹 캐시와 미러 서버 기술에 대해서 연구할 것이다. 그리고 공격자들이 웹 서버를 통한 트래픽을 증가시키는 동안, 이 기술들이 웹 서비스의 질을 유지시키고, 웹 서버 능력을 증가시킬 수 있는 능력을 제공 하는 지에 대해 검토할 것이다.

4.1 웹 캐시 서버

웹 캐시 서버는 요청한 내용을 알기 위해 서버와 사용자 사이에 위치한다. 한번 요청된 콘텐츠가 캐시 서버에 들어가면, 캐시 서버는 데이터베이스를 조사하여 만약 요청된 콘텐츠가 발견된다면, 저장하고 있던 복사본을 사용자에게 전달하고, 만약 그렇지 않으면 요청된 콘텐츠를 원래 웹 서버로 전달한다. 따라서 캐시 서버의 이용은 웹 서버 부하가 감소하고 요청되어지는 전체 네트워크에 대한 트래픽이 줄어들어 더 빠르게 응답을 할 수 있게 된다.[9].

캐시 서버에서 요청받는 콘텐츠는 복사본이 발견되어 지지 않거나, 저장된 콘텐츠를 업데이트 할 때 고려해야 할 문제점이 있다.

우선 성능은 중요한 문제이다. 정기적으로 콘텐츠를 캐시 서버에 복사하고, 다른 요청을 원래 서버에 전달하는 때에 속도를 고려해 보자.

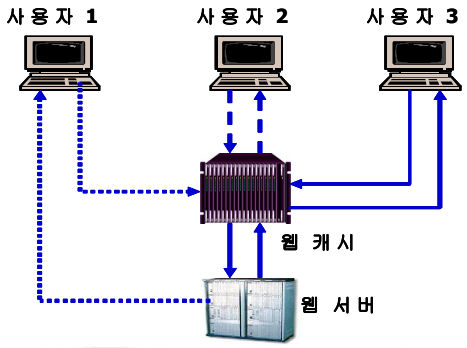

그림 7. 웹 캐시 사용
Fig. 7 Using of Web Cache

(그림 7)에서 사용자가 다른 서버들로부터 콘텐츠를 어디로 요청하는지, 그리고 캐시 서버는 이를 어떻게 처리하는지 3가지의 경우를 설정한다.

사용자 1의 경우 캐시 서버는 정적인 데이터베이스를 가진다. 그리고 요청받은 콘텐츠가 캐시 서버에 없을 경우 캐시 서버에서는 아무 일도 일어나지 않고 웹 서버에서 콘텐츠를 공급 받는다.

사용자 2의 경우 캐시 서버의 데이터베이스는 동적이다. 동적이란 것은 요청받은 콘텐츠를 찾지 못하면 콘텐츠를 복사하여 스스로 업데이트 하는 것을 의미한다. 만약 사용자에 의해 요청받은 콘텐츠가 캐시 서버에서 발견되면 복사해 두었던 콘텐츠를 쉽게 사용자에게로 전달한다.

사용자 3의 경우 캐시 서버의 데이터베이스는 동적이다. 요청받는 콘텐츠가 발견되지 않았다면, 캐시 서버는 원래 서버로부터 내용을 요청하고, 그 콘텐츠를 사용자에게 전달하기 전에 캐시 서버에 복사하여 업데이트 한다. 그리고 콘텐츠를 웹 캐시에서 복사 받아 사용자 3에게 제공한다.

4.2 미러 서버

미러 서버의 사용은 웹 캐시를 이용한 웹 서버보다 콘텐츠와 접속 빈도수가 월등히 많고, 동시 접속수가 많으며, 사용자의 이용 빈도가 높을 경우에 성능을 향상시키기 위해 설계된다.[10].

(그림 8)에서 미러 서버는 웹 서버에서 콘텐츠를 모두 복사하여 저장하거나, 웹 사이트에서 가장 인기 있는 빈도수가 높은 콘텐츠만을 선별적으로 저장한다. 따라서 콘텐츠를 미러 서버가 가지고 있을 때에는 미러 서버로 사용자의 네트워크의 경로 재지정(redirection) 된다.[11]. 이것이 캐시 서버와 다른 점이다.

미러 서버는 운영에는 사용자의 요구 사항 및 접속 빈도 분석을 통해 사용자를 분류하여 사용자의 접속 빈도에 따른 미러 서버를 여러 개로 운영 할 수 있다. 또한 접속 콘텐츠도 등급별로 분류되어 사용자의 있다.

미러 서버에 관한 네트워크 액세스 전략은 네트워크 경로 게이트웨이 재지정 과 자동 재지정, 두 가지가 있다. 게이트웨이 재지정의 경우, 사용자가 게이트웨이 웹 사이트에 접속하고 원하는 콘텐츠를 가지고 있는 미러 서버를 리스트에서 선택한다.[12].

게이트웨이 재지정을 사용하면 미러 서버가 주어진 데이터의 아이템 전체를 처리에 처리 용량이 증가한다. 하지만 접속빈도가 많고, 대용량의 콘텐츠을 요구하더라도 안정성 있게 처리하여 사용자들에게 최선의 선택을 하게 돕는다. 최적의 미러 서버의 트래픽 문제는 서버의 현재 트래픽 부하 상태에 비례한다.

서버의 트래픽은 요청 자료에 따라 변한다. 이를 반영한 좀 더 효율적인 경로 재지정은 가장 효율적인 방법으로 사용자의 요청을 분산하는 자동 재지정이다. 이를 적용한 것에는 CDN(Content Delivery Network)이 있다. CDN은 캐시 역할을 할 수 있도록 전체 네트워크 상에 동일한 콘텐츠 내용을 복제하여 대규모 인트라넷 또는 인터넷상에 분산시켜 놓은 시스템이다. 이를 통해 특정 지역 또는 전체 네트워크에 걸쳐 콘텐츠가 분산 배치되면, 사용자들은 훨씬 더 빠르게 콘텐츠를 볼 수 있다.

CDN은 사용자의 콘텐츠 요청에 반응하여, 원하는 내용을 찾아 경로 자동 재지정을 통해서 콘텐츠를 찾아 공급한다.

서버의 내용에 대한 요청은 자동적으로 미러 서버를 통해 분산되어진다. 각각의 서버는 단지 모든 요 청의 부분을 보고 빈번한 콘텐츠는 더 빠르게 저장한다.

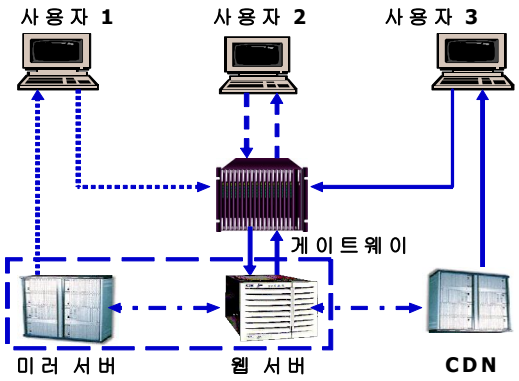

그림 8. 미러 서버와 CDN 사용
Fig. 8 Using of Mirror Server and CDN

(그림 8)에서 사용자 1이 요청한 콘텐츠는 접속 빈도수가 많은 내용으로 분류되어 있어 사용자가 선택 하자마자 게이트웨이에서 경로 재 지정을 통해 즉시 미러 서버에서 콘텐츠를 제공 받는다. 사용자 2는 사용자 1이 미러 서버를 사용하고 있으므로, 만약 같은 내용을 선택하면 미러 서버의 트래픽이 걸린다고 판단되면 웹 서버로부터 콘텐츠를 제공 받는다. 사용자 3은 게이트웨이에서 멀리 떨어진 곳에서 콘텐츠를 요청하여 경로 자동 재지정[13] 을 통해 가까운 CDN으로부터 콘텐츠를 제공받게 한다. 특히 자동 재지정은 네트워크의 트래픽에 따라 유연하게 미러 서버나 CDN 그리고 다른 미러 서버를 통해서 콘텐츠를 제공 받는다.

사용자의 콘텐츠 요청은 각각의 콘텐츠의 내용 접속 빈도수나 위치 및 트래픽에 기초한 콘텐츠 분산을 고려하여 사용자에게 가장 가까운 미러 서버나 CDN으로 보낸다. 그리고 게이트웨이에서의 네트워크 경로 재지정과 경로 자동 재지정은 웹 서버의 서비스 속도를 빠르게 하고, 네트워크에서 패킷이 머무는 시간을 줄여 트래픽을 줄인다.

V. 결론

초고속 통신이 발달하고 인터넷 이용률의 증가와 함께 지식 정보 산업화가 사회 전반으로 진행되고 있다. 따라서 네트워크가 차지하는 역할이 커지면서 네트워크 트래픽 문제

나 폭주로 인한 서비스의 마비는 정보보안에서의 중요한 요건이 되고 있다.

이 논문에서 우리는 TCP/IP의 취약점을 이용하여 네트워크 상에서 트래픽을 일으키는 원인에 대해 연구를 하였다. 그리고 DoS 공격 및 DDoS 공격, Sniffering 공격, Buffer Overflow를 이용한 공격, Smurfing을 이용한 공격, Land Attack, SYN Flooding을 이용한 공격, IP Fragment 공격, IP Spoofing 공격, Flash-Crowds, Teardrop 공격, New Teardrop/Bonk/Boink 공격 등을 연구 하였다.

그리고 이 공격들에 대비하여 방어하는 보안 방법으로는 패킷필터링과 콘텐츠 배분방법의 기술을 제안하였다. 패킷필터링의 방법은 네트워크 레벨 라우터에서 실행과 게이트웨이 레벨의 방화벽을 이용하는 방법, 그리고 응용계층 레벨에서의 프락시 서버를 이용하는 방법 등을 연구하였다. 또한 웹 서버에서의 콘텐츠 배분방법으로 캐시 서버를 이용하는 방법과 미러 서버와 CDN을 사용하여 콘텐츠를 분배하는 방법에 대해 연구 하였다.

이러한 제안들은 실제로 인터넷을 이용하는 사용자들과 콘텐츠 공급자들의 네트워크 트래픽을 줄이고, 공격자의 공격에 대응하는 방법으로 활용되어질 것이다.

향후 연구로는 유선뿐만 아니라 발달하고 있는 무선 분야의 이동 단말기를 통한 이동통신의 네트워크 보안과, 무선통신 트래픽 및 콘텐츠 배분에 관한 분산 기술 연구가 필요하다.

참고문헌

[1] Verm Paxson. An Analysis of Using Reflector for Distribueted Dinaial of Service Attacks. Computer Communication Reviwer. 2002.12.31.

[2] Steven Gibson. DRDOS Distributed Reflection Denail of Sevice February, 2002. http://grc.com/dos/drdos.html.

[3] 이준택, 배준호, 박미영, “Securing Network & Building Firewall.” 가남사, pp126-154, 2002. 4.

[4] W. Stallings, “Cryptography and Network Security.” Principles and Practice. Third Edition, Prentice -Hall, 2005.

[5] W. R. Cheswick and S. M. Bellovin. “Firewalls and Internet Security.” AT&T Bell Laboratories, Second Edition, 2003.

[6] 박대우, “32비트와 64비트 K4 방화벽 성능비교에 관한 연구.” 한국컴퓨터정보학회논문지, 제8권 제1호, pp30-36, 2003. 3. 31.

[7] 박대우, “외부 이동단말의 접근제어를 위한 IP 프로토콜 설계 및 성능 개선에 관한 연구.” 한국컴퓨터정보학회논문지, 제9권 제2호, pp41-48, 2004. 6. 30.

[8] 박대우, “Solalis K4방화벽에 대한 기능별 운영체제(32비트, 64비트)별 성능비교연구.” 한국통신학회논문지, 제28권 제12B호, pp1091-1099, 2003. 12. 30.

[9] H.Yu, L.Breslau, and S.Shenker, “A scalable web cache consistency architecture”, Proc. of ACM SIGCOMM, Sep. 1999.

[10] S.Jamin, C.Jin, A.R.Kurc, D Raz, and L.Zhang, “On the placement of internet instrumentation”, Proc. of IEEE INFOCOM, March 2000.

[11] Erbil Yilmaz, and Yanet Manzano. “Surveying formal and practical approaches for Optimal Placement of Peplicas on the Web, “TR-02071, Department of Computer Science, Florida State University, April 2002.

[12] A. Myers, P. Dinda, and H. Zhang, “Performance characteristic of mirror services on the internet,” Proc. of IEEE INFOCOM, March 1999.

[13] Yanet Manzano, “Filtering, and Content Distribution Approaches to Mitigate the Effects of DOS Attacks and Flash Crowds on Network Performance“, Cybernetics and Informatics (SCI2003), July 2003.

저 자 소 개

박 대 우

1987년 서울시립대학교 경영학과 졸업 (경영학사)
1995년 숭실대학교 컴퓨터학부 (컴퓨터부전공)
1998년 숭실대학교 컴퓨터학과 졸업 (공학석사)
2004년 숭실대학교 컴퓨터학과 졸업 (공학박사)
2000년 매직캐슬정보통신 연구소 소장, 부사장
2003년 숭실대학교 겸임조교수
<관심분야> 유비쿼터스, 인터넷S/W, 보안 S/W, 컴퓨터 및 네트워크 보안, 정보 보안, 이동통신 및 IMT-2000 보안, Cyber Reality

서 정 만

2003년 2월 충북대학교 컴퓨터공학과 공학박사
2002년~현재 한국재활복지 대학 컴퓨터게임개발과 교수
<관심분야> 데이터베이스, 게임프로그래밍, 실시간처리