한국산학기술학회논문지
Vol. 5, No. 5, pp. 447-453, 2004

인터넷 트래픽 제어에 관한 연구: IP 주소 위조 기법을 사용한 유해 정보 차단 시스템

백 선 욱*

A Study on Internet Traffic Control: Blocking of harmful information based on IP spoofing

Seon-uck Paek

요 약 본 논문에서는 사용자가 유해한 사이트에 접근하는 것을 효과적으로 방해하는 새로운 유해 정보 차단 시스템을 제안한다. 본 차단 서버 시스템은 설치된 망의 외부로 전송되는 모든 트래픽의 URL 정보를 감시하다가 외부의 유해한 사이트에 접속을 시도하는 내부 사용자를 발견하면 마치 유해 사이트로부터의 응답인 것처럼 위조된 TCP RST 세그먼트를 그 사용자에게 전송하여 사용자가 스스로 접속을 포기하도록 유도하는 IP 주소 위조(IP spoofing)기술을 사용하였다. 본 차단 시스템은 망 내부의 각 사용자 시스템에는 유해 정보 차단과 관련된 소프트웨어를 설치할 필요가 없이 하나의 서버에만 설치하면 되므로 쉽게 설치 및 유지 보수가 가능하다. 또한, 정상적인 트래픽 흐름에는 거의 영향을 미치지 않는 장점이 있다. 본 시스템의 성능을 측정하여 평가하여 본 결과 적정 규모의 네트워크에서 좋은 차단률을 보임을 확인하였다. 제안된 시스템은 IP spoofing 기법에 기반하고 있으므로 정상적인 접속요청도 방해하는 해킹 도구로 악용될 수 도 있는데, 이러한 가능성을 예방할 수 있는 방안도 함께 제안하였다.

Abstract In this paper, we propose a new system to block harmful Internet information based on IP spoofing. The proposed system is located on a organization's internal network and monitors all outgoing traffic and lets all this traffic go outside. Once the proposed system detects a host's access to a harmful site, it sends the host a pseudo RST packet that pretends to be the response from the harmful site, and prevents the connection between the host and the harmful site. The proposed software system is installed on only a server, and need not be installed on user hosts at all. Thus we can maintain and upgrade the blocking system easily. The performance evaluation of the proposed system shows that it effectively blocks the access to the harmful sites. Since the proposed system is based on IP spoofing, it can be used badly as a hacking tool. Finally we propose some methods to eliminate this possibility.

Key Words : Harmful information, IP spoofing, Hacking

1. 서 론

최근에 인터넷이 급속도로 보급되면서 가정 내의 청소년들이 성인들만 볼 수 있는 사이트나 혹은 폭력, 마약, 자살 등의 정보와 관련된 유해 사이트에 쉽게 접근할 수 있게 되어 사회 문제가 되고 있다. 또한, 일반 회사에서도 근무 시간에 근무와 무관한 사이트에 접근하여 업무 효율을 저하시키는 일들이 문제가 되고 있다. 이와 같은 유해 사이트에 사용자가 접근하는 것을 막기 위해 Cyber Patrol, Net Nanny, Cybersutter 및 에이지 시스템사의 모야, 플러스 기술의 수호천사, 인터정보사의 컴지기, Kids Cops 사의 키즈캅 등 여러 가지 시스템들이 개발되고 있는데 이러한 시스템들의 내부 동작 원리는 현재 자세하게 알려져 있지 않은 실정이다. 이러한 유해 정보 차단 시스템들은 설치 위치에 따라 크게 차단 소프트웨어를 사용자 시스템에 설치해야 하는 방식과, 차단 서버에 설치하는 방식, 혹은 사용자 시스템과 차단 서버 양쪽에 설치하여 상호 협력하는 방식 등으로 분류할 수 있다[1-3]. 이 중에서 사용자 시스템에 차단 소프트웨어 설치가 필요한 시스템은 차단 소프트웨어의 설치 및 유지 보수가 번거롭고 또한 노련한 사용자라면 자신의 시스템에 설치된 차단 관련 소프트웨어를 삭제할 수 있다는 문제점이 있다. 이에 본 논문에서는 사용자 시스템에 별도로 차단 소프트웨어를 설

*상명대학교 컴퓨터소프트웨어 전공

치하지 않고 차단 서버에만 차단 소프트웨어를 설치하여 유해 정보 차단을 할 수 있도록 한 차단 시스템을 개발하였다. 또한, 차단 서버에만 차단 소프트웨어를 두는 시스템 중에서 사용자로부터 유해 사이트로 향하는 패킷을 일단 버퍼에 저장해 둔 다음에 그 패킷에 있는 URL이 유해한 사이트로의 접근이라고 판단되면 차단하고 그렇지 않으면 외부로 패킷을 전달하는 방식은 유해하지 않은 사이트로의 트래픽도 모두 차단 서버의 검사를 거쳐야만 외부로의 전송이 가능하므로 차단 서버에서 병목 현상이 발생할 수 있다[1,2,7,8]. 본 논문에서는 일단은 모든 패킷이 외부로 나갈 수 있도록 허용하되 유해한 사이트로의 접속을 시도하는 사용자에 대해서만 접속을 방해하는 방식의 새로운 차단 시스템을 제안한다. 제안된 시스템은 정상적인 트래픽 흐름에 영향을 거의 미치지 않으면서 필요할 때만 IP 주소 위조(IP Spoofing) 기법[4]을 사용하여 차단을 하도록 하였다. 본 시스템은 Linux 환경에서 응용 프로그램 형태로 개발이 되어 이식성이 높으며, 커널에서의 필터링을 지원하는 pcap 라이브러리[5]를 사용함으로써 프로그램의 수행 속도를 향상시켰다.

본 논문의 2절에서는 유해 정보 차단과 관련된 기술을 살펴보고 3절에서는 제안된 차단 시스템의 원리와 구조 및 특징을 기술한다. 4절에서는 개발된 차단 시스템의 악용 가능성을 방지하는 기법에 대해 서술하고 5절에서는 개발된 시스템의 성능 측정 결과를 논한다.

2. 관련 연구 동향

유해 정보 차단 시스템은 다음과 같은 기준에 의해 분류할 수 있다.

2.1 차단 정보 관리 방법에 의한 분류:

"차단 목록 기반의 여과(Black List Filtering)" 기술과 "허용 목록 기반의 여과(White List Filtering)" 기술 및 "부여등급 기반의 여과(Neutral Label Filtering)" 기술로 분류할 수 있다[1-3,6].

먼저, 차단 목록 기반의 여과(Black List Filtering)에서는 차단 목록에 있는 사이트로의 접근만 차단하고 그 외의 사이트에 대한 차단은 허용하는 방식으로 현재 대부분의 접속 차단 시스템이 이런 구조를 사용하고 있다. 반면에 허용목록 기반의 여과(White List Filtering) 방식은 허용 목록에 있는 사이트로의 접근만 허용하고 그 외에는 접근을 거부하는 방식이다. 마지막으로 부여 등급 기반의 여과(Neutral Label Filtering) 방식은 인터넷 상의 정보에 대해 일정 기준에 의해 등급을 부여한 뒤에 일정 등급 이상의 정보에 대한 접근은 차단하는 방식이다. 대표적으로 PICS(Platform for Internet Contents Selection)에 의한 등급표시방법을 들 수 있다[6]. 본 논문에서 제안하고 있는 시스템은 차단 목록 기반의 차단 방식에 속한다.

2.2 차단 위치에 의한 분류:

클라이언트에서 차단하는 방식과 라우터나 프락시 서버에서 차단하는 방식으로 분류할 수 있다. 클라이언트에서 차단하는 방식은 PC 등 웹브라우저가 설치된 클라이언트에서 차단하는 방식으로 인터넷 접속이 가능한 모든 단말기에 차단 프로그램을 설치해야 하므로 유지, 보수가 쉽지 않으며 또한 차단 프로그램의 비정상적인 삭제 등에 대한 대비책이 필요하다. 반면에 라우터나 프락시 서버에서의 차단 방식은 대부분 그림 1과 같이 게이트웨이나 라우터 혹은 별도의 서버에 프락시(proxy) 방식의 차단 프로그램을 설치하는 방식이다[1-2,7,8].

망 내부로부터 외부로 향하는 트래픽은 일단 차단 프락시에서 차단 목록 데이터베이스와의 비교를 거쳐야 하며, 차단 목록에 없는 트래픽만 망 외부로 전달되고 그렇지 않은 트래픽은 망 외부로 전달되지 않는다. 여기서 차단 목록은 별도의 외부 데이터베이스 서버 형태로 설치할 수도 있다. 이 방식에서는 인터넷 접속은 유해한 사이트로의 접속이든 유해하지 않은 사이트로의 접속이든 반드시 차단 proxy를 반드시 통해야 외부 망으로의 접속 허용 여부가 결정되므로 망의 부하가 높아지면 차단 프락시가 병목 현상을 일으켜 정상적인 인터넷 사용자에게도 성능 저하를 초래할 수 있다. 본 논문에서는 차단 프락시를 사용하지 않는 새로운 유해 정보 차단 시스템을 제안하는데, 제안된 시스템은 정상적인 사용자의 트래픽 성능에 거의 영향을 미치지 않으면서도 효과적으로 유해 정보 접속을 차단할 수 있도록 하였다.

3. 차단 시스템 구조

본 논문에서 개발한 차단 서버 시스템의 위치는 그림 2

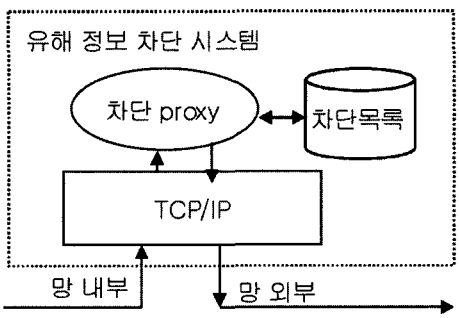

Fig. 1. proxy 방식의 유해 정보 차단 시스템.

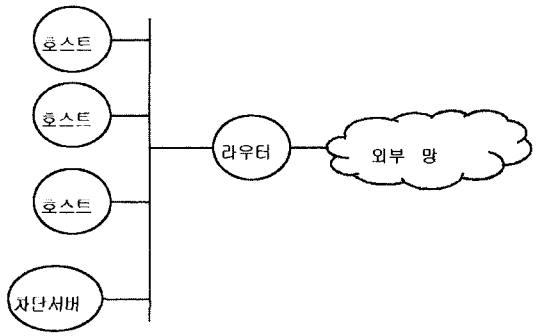

Fig. 2. 차단 서버의 위치.

와 같이 조직이나 기관 내의 망 내에서 외부로 전송되는 모든 패킷을 감시할 수 있는 위치라면 어느 곳이라도 관계없다. Ethernet에서는 promiscuous 모드로 차단 서버를 설정해 두면 망 내의 모든 트래픽을 감시할 수 있다.

본 논문에서 제안하고 있는 차단 서버는 [1,2,7,8]의 프락시 방식의 차단 서버와 달리 외부로 나가는 트래픽을 저장해 두지 않고 망 외부로 모두 나가도록 일단은 허용하도록 하되, 그 트래픽의 URL을 분석한다. 만일 유해 사이트로의 접속 요청이라고 판단되면 외부의 유해 사이트가 접속을 거부한 것처럼 IP 주소를 위조한 RST(Reset) 세그먼트를 그 URL로의 접속을 시도한 사용자에게 전송하여 클라이언트로 하여금 스스로 연결을 종료하도록 유도하였다.

그림 3은 차단 서버에서 위조 RST 세그먼트를 보내는 시점을 보여주고 있다. http 프로토콜에서는 내부 사용자 호스트와 외부의 웹서버가 연결을 설정하기 위해 필요한 3-way handshake 과정[8]이 끝난 후에 사용자 호스트가 HTTP GET 요청 메시지를 보내게 되는데, 본 차단 시스템에서는 이 세그먼트에서 추출한 URL을 가지고 차단 서버가 관리하고 있는 유해 사이트 목록(차단 목록) 데이터베이스에서 검색해서 유해한 사이트로의

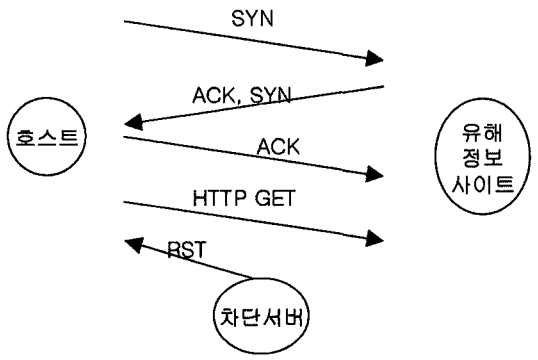

Fig. 3. 연결 차단 구조.

접속시도인지 아닌지를 판단한다. 분석결과 유해한 사이트로의 접속 시도라고 판단되면 차단 서버는 IP 주소를 유해 정보사이트의 주소로 위조한 RST(Reset) 세그먼트를 해당 사용자에게 전송하여 연결 해제를 시도한다. 사용자로부터 GET 요청을 받은 외부의 유해 사이트도 이 요청에 대응하는 응답 메시지를 보내지만 내부 사용자와 가까이 있는 차단 서버로부터의 위조 RST 세그먼트가 대부분 먼저 도착하게 되므로 유해 정보 차단이 가능하다.

이 방식에서는 프락시 방식의 차단 시스템과 달리 외부로의 모든 트래픽을 일단 저장해 둘 필요가 없으므로 망에 부하가 많더라도 차단 서버가 병목현상이 되지 않는 장점이 있다.

여기서 차단 서버가 사용자(호스트)를 속이는 것은 위조 RST 세그먼트의 IP 주소와 TCP sequence 번호 및 포트 번호들을 *http GET* 메시지의 값들과 일치시켜 주면 가능하다. 즉, 차단 서버가 전송하는 위조 RST 세그먼트에는 원래 사용자가 접속하고자 했던 유해 사이트의 IP 주소, sequence 번호, 포트 번호를 적어 넣어 위조하며, 이렇게 위조된 세그먼트를 수신한 사용자는 이것들이 원래의 서버로부터 온 것으로 간주하여 연결을 종료하게 된다[4][9]. 여기서 연결을 방해하기 위한 목적으로 TCP의 위조 FIN(Finish) 세그먼트를 사용자에게 전송하는 것도 고려해 볼 수 있는데, 실제로 실험결과 이 경우에는 사용자 호스트와 유해 사이트 서버가 연결 해제를 위한 3 way handshake 과정에 진입함으로써 여러 번의 세그먼트 교환이 추가로 유발되어 망에 트래픽 부하를 증가시키는 문제점이 있다[9]. 반면에 본 시스템에서처럼 TCP의 RST 세그먼트를 전송하는 경우에는 추가적인 세그먼트를 생성시키지 않는 장점이 있다. 이 외에도 ICMP 프로토콜의 Destination Unreachable 메시지 중에서 여러 가지 code 값을 갖는 메시지를 위조해 보는 것도 검토해 볼 수 있고, Time Exceed, Parameter Problem 메시지 등을 사용하는 것도 검토해 볼 수 있다. 위에 나열한 RST, FIN, ICMP 메시지에 실제로 사용자 호스트가 어떤 응답을 보일지는 사용자 호스트가 사용하고 있는 운영체제에 따라 약간씩 다를 것으로 예상된다. 본 논문에서는 사용자 호스트로 linux를 사용하였다.

본 시스템에서는 SYN(Synchronize) 세그먼트에 있는 IP 주소만을 보고 차단 여부를 결정하지 않고 3-way handshake에 의한 연결 설정이 완성된 다음에 사용자가 전송하는 GET 요청 메시지의 내용(URL)을 살펴보고 차단 여부를 결정하도록 하였다. 그 이유는 내부의 호스트가 유해 사이트와 직접 연결하지 않고 유해하지 않다고 판단된 외부의 서버(proxy server)를 경유하여 접

속하는 경우도 차단하기 위해서이다. 이렇게 외부의 서버를 경유하는 경우의 SYN 세그먼트에는 외부의 경유 서버의 IP 주소만 나타나게 되므로 이 IP 주소만으로 유해성 여부를 판단하면 정확한 판단이 되지 않을 수도 있다. 반면에 외부의 경유 서버와의 연결 요청이 완성된 이후에 그 경유 서버로 전달되는 GET 요청에는 최종적으로 접속하고자 하는 유해 사이트의 URL 정보가 포함될 수밖에 없으므로 이 정보를 가지고 데이터베이스를 검색하면 보다 정확한 차단 기능이 가능해진다. 사용자가 바로 유해 사이트에 접속하는 경우에는 GET 요청에 디렉토리 이름이 나타나게 되며, 외부의 서버를 경유하는 경우에는 GET 요청 메시지에 최종 목적지의 URL이 나타나게 된다. 또한 이렇게 GET 요청 세그먼트를 보고 차단 여부를 결정하는 것은 단순히 IP 주소 수준에서 차단을 결정하는 것이 아니라 서버 내의 각 디렉토리 수준에서 차단 여부를 결정하는 것이 가능하게 되어 보다 정교한 차단 제어가 가능해진다. 또한, 접속을 시도한 사용자 호스트에게 때로는 경고 메시지를 넣은 html 문서를 보낼 필요가 있는데, 이러한 html 문서의 전송은 3-way handshake가 완성된 다음이라야 가능하다.

여기서 차단 서버가 접속을 끊기 위해 보내는 위조 RST 세그먼트가 외부의 실제 유해 사이트로부터의 응답보다 늦게 사용자에게 전달될 경우에는 차단이 일시적으로 늦어질 수가 있는데, 그렇다 하더라도 사용자의 지속적인 유해 사이트 연결은 방해할 수 있으므로 소기의 목적은 달성할 수 있다. 실제로 위조 RST 세그먼트를 전송하여 연결을 끊기 전에 먼저 경고 메시지를 담은 html 문서를 사용자 호스트로 전송하도록 구현하여 사용자로 하여금 차단 서버가 동작하고 있음을 인식할 수 있도록 하여 더 이상의 시도를 꺼리도록 하였다.

본 시스템에서 유해 차단 서버로는 linux를 사용하고 유해 목록 저장을 위한 데이터베이스로는 http://Hughes.com.au 에서 제공하고 있는 mSQL[10]을 사용하였으며, 차단 서버가 망의 트랙픽 흐름을 감시할 수 있도록 하기 위한 필터링 도구로는 pcap 라이브러리를 사용하였다[5]. pcap 라이브러를 통해 검사하고자 하는 패킷을 응용 계층으로 불러올 수 있는데, 본 논문에서는 http 트래픽만 감시하고자 하였으므로 목적지 포트 번호가 80번인 패킷만을 선별하도록 하여 차단 서버에 대한 부하를 최소화하고자 하였다. 만일 ftp 등의 다른 서비스도 차단하고 싶으면 해당 서비스 번호에 해당하는 패킷들도 pcap이 수신하도록 하면 된다. 또한 유해한 서버로의 접근이라고 판단되어 IP spoofing 기법을 사용한 모조 패킷을 전송하기 위해서는 socket 라이브러리의 raw socket 기능을 이용하였다.

4. 차단 서버의 오용 방지 기법

본 논문에서 제안하고 있는 차단 서버는 IP spoofing 기법에 기반하고 있으므로 악용될 경우 망을 마비시키는 강력한 해킹 도구로 사용될 수 있다. 즉, 해커가 본 차단 서버를 망 내에 몰래 설치한 다음에 외부로의 접속을 시도하는 모든 사용자 연결 요청에 대해 접속을 방해하는 위조 RST 세그먼트를 발송한다면 그 망 내부의 모든 사용자들은 정상적인 인터넷 서비스를 받을 수 없을 것이다. 이런 경우를 대비하여 본 논문에서는 차단 서버의 이러한 악용을 막을 수 있는 보완책을 제시하는데, 차단 서버와 라우터 및 각 사용자 시스템의 상호 협조를 필요로 한다.

먼저, 해킹 시스템이 망 내에 있으면서 위조 RST 세그먼트의 MAC 주소를 원래의 차단 서버의 주소로 위장하는 경우에는 차단 서버가 탐지해 낼 수 있다. 또한, 해킹 시스템이 망 내에 있으면서 위조 RST 세그먼트의 MAC 주소를 라우터의 MAC 주소로 위장한 경우에는 라우터가 검출해 낼 수 있다. 그리고 MAC spoofing은 하지 않고 단순히 IP spoofing 만 하는 경우에는 망 내에 있는 호스트들의(MAC 주소, IP 주소) 쌍에 관한 정보를 차단 서버나 라우터가 갖고 있다가 전송되고 있는 세그먼트 헤더에 있는 MAC 주소와 IP 주소의 일치 여부를 검사함으로써 탐지해 낼 수 있다.

그러나 본 논문에서 차단 서버가 망의 외부에 위치하면서 사용자가 접속하고자 하는 서버의 IP 주소로 위장하는 경우에는 전술한 방식으로는 검출할 수가 없으며, 별도의 인증 기능이 사용되어야 함께 하는데, 예를 들어 IPsec의 AH 기능을 활용하는 방안을 고려해 볼 수 있다[8].

5. 성능 평가

2절에서 서술한 프락시 방식의 차단 시스템에서는 외부로의 트래픽을 일단 차단 프락시에서 저장하여 유해성 여부를 검사한 다음에만 외부로의 접속을 허용하므로 차단 목록 데이터베이스에 있는 사이트로의 접근은 100% 차단될 수 있다. 그러나 본 논문에서는 이러한 프락시 방식과 달리 일단은 외부로의 모든 트래픽이 모두 외부로 나가는 것을 허용하되, 유해한 사이트로의 접속 시도만 IP spoofing을 사용하여 차단하므로 만일 망 외부의 유해 사이트로부터의 응답이 위조 RST 세그먼트보다 먼저 도착했을 경우에는 초기 차단이 실패할 수도 있다. 이에 본 논문에서는 망 외부에 있는 유해 사이트에 접속하려고 할 경우에 본 차단 시스템을 적용했을 경우의 초기 차단 성공률을 조사하였다. 이를 위해

TCP의 연결 접속 요청 세그먼트인 SYN 세그먼트를 연속해서 전송하도록 한 에뮬레이터를 linux에서 작성하였다. 차단 서버와 네트워크 에뮬레이터는 동시 사용자가 200명 규모인 회사의 내부의 10 Mbps LAN에 접속 설치하였으며, 시스템 사양으로는 둘 다 PC 급 호스트를 사용하였다. 이 에뮬레이터를 이용하여 유해 사이트라고 가정한 사이트로 SYN을 100, 200, 300개를 연속해서 전송하여 연결 설정을 시도하도록 하였다. 그 다음에 차단 서버를 운용하여 유해 사이트로부터의 응답 메시지보다 차단 서버로부터의 위조 RST 응답이 먼저 에뮬레이터에 수신되는 경우의 비율을 계산하였다.

실제 실험 환경에서는 외부 인터넷 망의 트래픽 부하 상황 변화를 일정하게 유지할 수 있는 방법이 없어서 실험 결과 연결 요청수와 차단성공율에 대한 결과값의 편차가 심하였다. 그러나 하루 중의 같은 시간대에 반복 실험하고, 또한, 차단 서버와 에뮬레이터를 별도의 분리된 망에 설치하여 실험함으로써 가능하면 외부 트래픽의 영향을 덜 받도록 하고자 하였다.

그림 4는 국외에 소재하고 있는 유해 사이트에 대한 접속 시도 결과를 보여주고 있다. 일반적으로 유해한 사이트에의 연결 요청수가 많아지면 차단 성공률도 낮아지며, 전체적으로는 거의 80% 이상의 초기 접속 차단률을 보여주고 있다. 또한 데이터베이스에 있는 유해 목록의 크기가 크면 일반적으로 데이터베이스 검색 시간이 더 걸려 차단율이 더 저하될 것으로 예측했는데, 실제 실험 결과 유해 목록의 크기에 대한 의존도는 그리 크지 않다고 보여진다.

또한, 본 논문에서는 간단한 mSQL을 데이터베이스로 사용하였으나 보다 우수한 성능을 지닌 상용 데이터베이스를 사용한다면 유해 정보 검색 시간의 영향을 더 감소시킬 수 있으리라 예상된다.

그림 5는 국내에 소재하고 있는 유해 사이트에 대한 접속 시도 결과를 보여주고 있다. 유해 사이트가 국외에 있는 경우에 비해 접속 차단률이 다소 떨어지는 것을 알 수 있는데, 그 이유는 원래의 유해 서버로부터 오는 응답시간이 국외인 경우보다 국내의 경우에 더 짧기 때문으로 추정된다. 또한 어떤 순간에는 국내 유해 사이트에 대한 접속 차단 성공률이 국외 유해 사이트에 대한 접속 차단 성공률보다 더 높은 경우도 가끔 발생하였는데, 그 이유는 유해 사이트로부터의 응답시간이 사용자 컴퓨터와 유해 사이트와의 지리적인 거리와 함께 접속을 시도할 당시의 외부 인터넷 망의 트래픽의 혼잡한 정도에도 크게 의존하기 때문이라고 판단된다.

그림 4과 5에서 알 수 있듯이 본 시스템은 기존의 트래픽 흐름에 영향을 주지 않으면서 위조 패킷을 전송하여 연결을 방해하는 방식이므로 연결 초기에 100% 차단하는 것은 가능하지 않다고 볼 수 있다. 그러나 이러한 점이 실제 유해 사이트 접속을 차단하는 데는 크게 문제가 되지 않는다. 즉, 차단 작업이 지연되어 유해 사이트로부터 사용자 호스트로 연결 초기에 유해 사이트의 일부 정보가 사용자 호스트에 전달 될 수 있으나 곧바로 차단 서버에 의한 RST 세그먼트에 의해 연결이 바로 단절된다. 예를 들어 완전 차단율이 80%라면 10개의 접속 시도 중 8개는 유해한 정보를 전혀 볼 수 없으며, 연결에 성공한 나머지 2개의 접속을 통해서는 유해한 정보가 일부 전달될 수도 있으나 곧 바로 RST 패

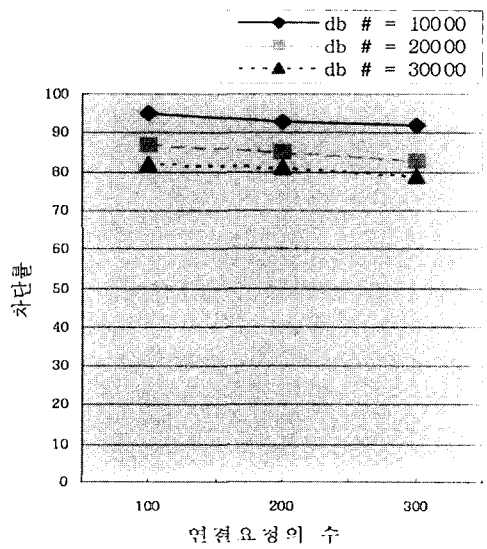

Fig. 4. 차단 서버의 성능(국외).

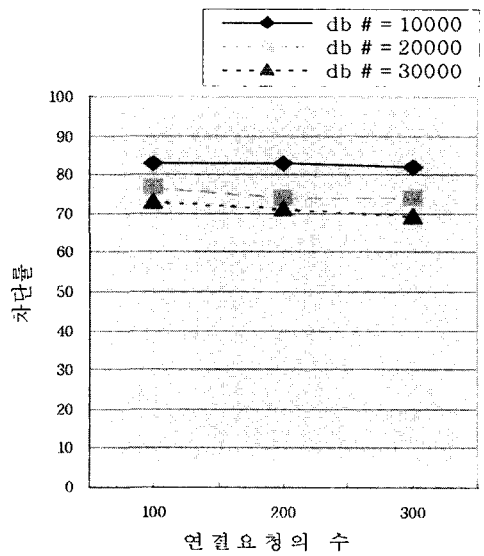

Fig. 5. 차단 서버의 성능(국내)

킷에 의해 나머지 유해 정보는 차단된다. 또한, 유해 사이트에 대한 접속을 시도한 호스트에 대해 경고 메시지를 보여주는 관리 정책 등에 의해 차단의 효과를 충분히 기대할 수 있기 때문이다. 이상의 실험 결과로부터 본 시스템은 대부분의 기관이나 조직에서 충분히 사용될 수 있으리라 예측된다. 게다가 본 시스템에서 사용한 PC급 차단 서버의 사양을 워크스테이션 급으로 개선한다면 더 나은 성능을 보일 것으로 기대된다. 또한, 이외에도 다양한 성능 향상 방법을 생각해 볼 수 있는데, mSQL보다 더 우수한 데이터베이스를 사용하거나 혹은 데이터베이스를 하드 디스크가 아니라 주기억장치에 두는 기법(In-memory DB)을 생각해 볼 수 있다. 또한 이중 CPU(dual CPU)를 채택하여 하나의 CPU는 차단 여부 검사만 하고 나머지 CPU는 모조 패킷을 만들어 전송하는 작업만 하도록 파이프라이닝 기법을 사용하는 방법 등을 고려하면 더 우수한 차단 성능을 기대할 수 있다.

6. 결 론

본 논문에서는 IP 주소 위조 기법에 기반한 유해 정보 접속 차단 시스템을 개발하였다. 차단 서버는 조직이나 기관의 망 내의 모든 트래픽을 감시할 수 있는 위치에 설치되어 외부의 유해 사이트에 연결을 시도하는 사용자를 발견하면 차단 서버는 마치 외부의 유해 사이트가 응답하는 것처럼 위장한 RST를 전송하여 접속이 끊어지도록 유도하였다. 본 시스템은 프락시 방식의 차단 서버와는 달리 기존의 정상적인 사용자의 트래픽에 영향을 거의 미치지 않으며, 또한 사용자 호스트에 별도의 차단 소프트웨어를 설치할 필요가 없다는 장점이 있다. 본 시스템의 차단율을 실험한 결과 유해 사이트로의 연결요청이 동시에 최대 300개까지 발생하여도 국외 유해 사이트는 80% 이상, 국내 유해 사이트는 거의 70% 이상의 차단률을 보이는 것을 알 수 있었다.

본 논문에서 제안하고 있는 차단 시스템은 정상적인 사용자의 접속도 차단할 수 있는 강력한 해킹도구로 사용될 수 있는데, 이를 막기 위한 기법들도 제안하였다.

본 논문에서 제안한 시스템이 효과적으로 동작하기 위해서는 차단 목록 데이터베이스를 어떻게 유지하고 갱신하는가 하는 것이 중요한 과제가 될 수 있는데, 이 문제는 웹 문서의 내용이나 그림을 자동적으로 검사하여 유해 목록 데이터베이스를 갱신하는 방식으로 나아가야 할 것으로 판단되는데, 예를 들어 [12-15]의 연구 결과를 활용한 시스템과의 연동을 통하여 해결방안을 모색할 필요가 있다. 또한, [16]에서는 차단 시스템의 성능을 향상시킬 목적으로 과거의 차단 결정을 캐쉬에 보관한 후에 DNS와 연계하는 방안을 제안하고 있는데, 이러한 속도 개선 분야에 관한 연구도 지속적으로 이루어져야 할 것으로 판단된다.

감사의 글

본 연구는 상명대학교의 교내연구비 지원에 의해 수행되었음.

참고문헌

[1] 서버용 유해정보 차단도구 개발 연구 보고서, 한국전산원, 1998.

[2] 유해정보 차단에 관한 기술지원 보고서, 한국전산원, 1998.

[3] 심재권, 김귀복, 박기홍, "유해정보의 경향과 유해정보 차단 소프트웨어의 문제점에 관한 연구", 한국정보과학회 2000 가을 학술발표논문집(I), pp. 638-640, 2000. 10.

[4] Chirillo John, Hack Attacks Encyclopedia, Wiley, 2001.

[5] PCAP Library, ftp://ftp.ee.lbl.gov/libpcap.tar.z Lawrence Berkeley Lab.

[6] http://www.w3.org/PICS/

[7] 박인성, 김홍철, 송병욱, 김상욱, "홈네트워크 환경에서 커널모듈을 이용한 유해사이트 차단", 한국정보과학회 2001 봄 학술발표논문집(A), pp. 781-783, 2001. 4.

[8] 김태웅, 류호연, 김성조, "RADIUS 서버를 이용한 사용자 인증 기반 URL 필터링 시스템의 설계 및 구현", 한국정보과학회 2003 춘계학술발표논문집, Vol. 30, No. 1, 2003. 4.

[9] TCP/IP Illustrated Volume I , 2 W. Richard Stevens, Addison-Wesley Publishing Company, 1996.

[10] mSQL, http://Hughes.com.au.

[11] S. Kent and R. Atkinson, IP Authentication Header, RFC2402, 1998.

[12] 육현규, 유병전, 박명순, "페이지 그룹 검색 모델: 음란성 유해 정보 색출 시스템을 위한 인터넷 정보 검색 모델", 한국 정보 과학회 논문지(A) 제 26권 제 12호, pp. 1516-1528, 1999. 12.

[13] 이병선, 정장호, 이은주, "유해 사이트 식별을 위한 칼라 영상에서 인체 검출", 정보과학회 2001 가을 학술발표논문집 II, pp. 352-354, 2001. 10.

[14] Keiichiri Hoashi, Naomi Inoue, and Kazuo Hashimoto, "Data Collection for Evaluating Automatic Filtering of Harzardous WWW Information", IEEE Internet Worksop 1999.

[15] Chen Ding, Chi-Hung Chi, Jing Deng, Chun-Lei Dong, "Centralized Content-Based Web Filtering and Blocking: How Far Can It go?", Proc. of 1999 IEEE

International Conference on Systems, Man and Cybernetics, Vol 2, pp. 115-119, October 1999.

[16] Chi-Hung and Henry Palit, "Two-layer Host Blocking: Caching the Blocking Decisions", Fifth International Conference on Algorithms and Architectures for Parallel Processing (ICA3PP'02) October 23-25, 2002 Beijing, China. p. 0464-0470.