사용자별 인증을 통한 웹 필터링 시스템 설계

전해식[0] 김성조
중앙대학교 컴퓨터 공학과
{hsjun, sjkim}@konan.cse.cau.ac.kr

Design of Web Filtering System through User Authentication

Hae-Sik Jun[0] Sung-Jo Kim
Dept. of Computer Science & Engineering, Chung-Ang University

요 약

예전에는 소수 사람들의 전유물로만 여겨졌던 인터넷을 이제는 가정주부나 어린이들까지도 쉽게 접근할 수 있을 정도로 보편화되었다. 이렇게 보편화된 인터넷은 우리의 생활을 윤택하게 해주는 다른 한편에서는 불법 음란물의 확산 및, 인터넷 중독과 같은 사회문제를 낳고 있다. 이로 인해서 웹 필터링 시스템의 사용이 늘어가고 있으나 이 웹 필터링 시스템 또한 광범위한 정보의 차단으로 인해 다른 사람들의 표현 및 정보공유의 자유를 침해한다는 주장이 나오고 있다. 본 논문에서는 이러한 문제를 해결하기 위한 해결책으로 사용자별 인증을 통한 필터링 시스템을 설계하였다.

1. 서 론

예전에는 소수 사람들의 전유물로 여겨졌던 인터넷이 이제는 학교나 회사뿐만 아니라 일반 가정주부나 어린이들까지 쉽게 접근하여 원하는 정보를 얻을 수 있을 정도로 확산되었다. 이러한 인터넷은 정보의 바다라고 불릴 정도로 엄청나게 많은 양의 정보를 제공하며, 또한 다른 사람들과의 커뮤니케이션을 원활하게 해 줌으로서 우리의 생활을 더욱 편하고 윤택하게 만들어 주고 있다. 그러나 이렇게 좋은 일면의 다른 한편에서는 이 확산된 인터넷으로 인한 여러 가지 사회적 문제를 야기 시키고 있다. 어린 학생들은 음란물, 마약, 폭력, 도박 등의 유해한 정보에 대해 무방비 상태로 노출되어 있으며, 회사에서는 직원들의 업무 외의 불필요한 인터넷 사용으로 인한 생산성 감소 및, 자원의 비효율적인 사용으로 인해 네트워크비용을 증가시키고 있다. 이러한 문제점들로 인해 학교나 회사, 가정에서는 인터넷의 유해정보를 차단하는 웹 필터링 소프트웨어를 설치하는 경우가 늘어가고 있다. 하지만 가정이나 학교에서 학생들에게 유해한 정보로부터 차단하기 위해서는 음란물, 마약과 같은 불법적인 정보뿐만 아니라 뉴스그룹, 채팅, 성인물과 같은 정보 또한 모두 차단하여야 하는데 이로 인해서 다른 성인들에게까지 표현 및 정보공유의 자유를 침해한다는 주장이 나오고 있다. 또한 회사에서는 증권, 신문, 방송과 같은 정보를 회사 전체에 대해서 차단함으로서 부서나, 직원의 특성상 필요한 정보를 같이 차단하게 되는 경우가 생기게 된다. 이러한 광범위한 정보의 차단으로 인해서 생기는 폐해를 줄이기 위해서는 모든 사람들에게 공통적으로 차단정책을 적용하는 것이 아니라 개인별 혹은 그룹단위로 차단 정책을 적용할 수 있는 방법이 필요하다. 본 논문에서는 이와 같이 개인별 혹은 그룹단위의 차단 정책을 적용할 수 있는 웹 필터링 시스템을 제안한다.

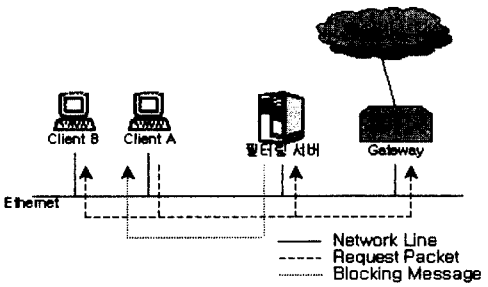
본 논문의 구성을 살펴보면 2장에서는 현재 나와 있는 필터링 방법에 대해서 살펴볼 것이며, 3장에서는 이 논문에서 제안하는 사용자별 인증을 통한 웹 필터링 시스템에 대해서 상세히 살펴볼 것이다. 마지막 4장에서는 결론 및 향후 연구 과제에 대해서 기술한다.

2. 필터링 시스템

네트워크 차원에서 유해 정보를 차단하기 위한 필터링 시스템은 크게 두 가지 카테고리로 분류할 수 있다. 첫 번째는 패킷 모니터링을 통하여 네트워크상에 지나가는 패킷을 분석하거나 스위칭 허브를 통하여 포워딩(forwarding)되어 들어오는 패킷을 분석하여 필터링을 하는 모니터링 방식이며, 두 번째는 네트워크의 게이트웨이(Gateway)를 통해서 나가는 요청을 게이트웨이 바로 앞에서 필터링 하는 게이트웨이 방식이 있다.

2.1 모니터링 방식

모니터링 방식은 네트워크 상에 브로드캐스팅되는 패킷이나 스위칭 허브에 의해서 포워딩되는 패킷을 필터링 서버가 분석하여 클라이언트에게 차단 메시지를 보냄으로서 필터링 하는 방법이다.



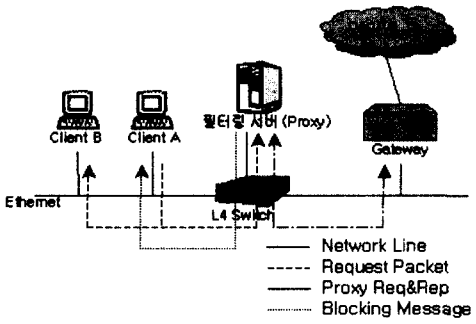
[그림 1] 모니터링 방식에 의한 필터링 시스템

[그림 1]은 이더넷 상에서 모니터링 방식이 적용된 하

나의 예이다. ClientA가 요청 패킷을 이더넷 상에 브로드캐스팅하면 필터링 서버는 이 패킷을 붙잡아 차단되어야 하는 패킷인지 아닌지를 판별하여 차단될 메시지인 경우에는 필터링 서버가 ClientA가 요청하고자 하는 원래의 서버인 듯 패킷을 모조 하여 ClientA에 ICMP[2]의 Destination Unreachable 메시지를 보냄으로서 패킷을 차단하는 방법이다. 이 방법은 필터링 서버에 대해서 투명성을 제공하여 주면서 외부로 나가는 패킷을 블록킹하지 않는 다는 특징을 가지고 있다.

2.2 게이트웨이 방식

게이트웨이 형태의 필터링 시스템 트워크의 트래픽을 어느 한 지점을 지나가게 구성한 다음에 그곳에서 패킷을 블록킹한후 차단 여·부를 판별하는 방식이다. 이와 같은 형태에서 대표적인 방법은 프록시(Proxy)[1,2]를 이용하여 필터링 시스템을 구성하는 것이다.



[그림 2] 프록시를 이용한 필터링 시스템

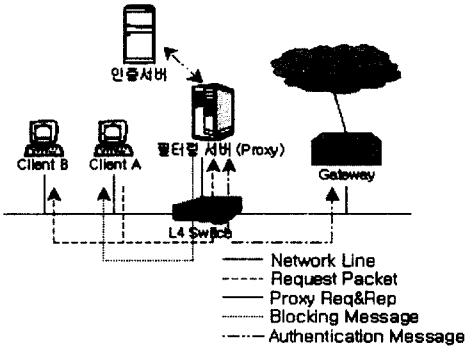
프록시를 이용한 필터링 시스템[1]은 [그림 2]에서 보이는 바와 같이 게이트웨이 바로 앞에 있는 Layer4 스위치에서 웹 요청에 해당하는 트래픽을 필터링 서버쪽으로 보내게 된다. 필터링 서버는 ClientA의 요청을 대신 받아서 차단 여·부를 판별한 다음 패스해야할 요청이면 프록시 서버 본연의 목적대로 원래의 서버에서 웹 페이지를 요청한 후 요청한 페이지가 오면 ClientA에게 전달한다. 만약 차단해야 할 요청인 경우에는 바로 ClientA에게 프록시 서버에서 HTTP[1]형식의 차단 메시지인 (Forbidden)를 보내게 된다. 프록시를 이용한 방법은 블록킹한후 차단 여·부를 판별하기 때문에 느리다고 생각할 수 있으나 서버 자체적으로 캐싱을 하고있기 때문에 성능적은 문제는 없어지게 된다. 또한 프록시 방식을 사용하면 요청되는 패킷만을 가지고 차단 여부를 판별할 뿐만 아니라 ClientA에게 보내지는 웹 페이지의 내용을 기반으로 차단하는 방법을 적용할 수도 있다.

3. 사용자별 인증을 통한 웹 필터링 시스템 설계

3.1. 시스템 설계

이 논문에서 제안하는 사용자별 인증을 통한 웹 필터링 시스템은 2.2절의 프록시를 이용한 필터링 시스템을 기본으로 하고 사용자 인증 시스템을 통합하는 방식으로 설계하였다. [그림 3]은 본 논문에서 제안하는 개인별 인증을 통한 웹 필터링 시스템을 보여주고 있다.

Layer4 스위치가 프록시 쪽으로 웹 요청을 보내게 되면 필터링 시스템은 요청이 온 클라이언트의 IP가 인증된 것인지 아닌지를 살펴본 후에 인증이 되지 않은 요청이라면 인증을 하기 위한 과정을 거치게 된다.



[그림 3] 사용자별 인증을 통한 필터링 시스템

사용자별 인증을 하기 위해서는 웹 요청을 하는 사용자와의 인터렉션이 필요하게되는데 이것을 쉽게 하기위해서는 사용자의 요청에 대해서 응답을 하거나 사용자의 요청을 블록킹하고 데이터를 처리할 수 있어야 한다. 2.1절에서 살펴본 모니터링 방식의 필터링 시스템은 사용자의 요청에 대해서 응답하기가 쉽지 않다. 사용자 인증을 위해서는 HTML형식의 사용자 인터페이스를 필요로 하는데 모니터링 방식은 클라이언트에게 웹 페이지를 보내기가 힘들며 또한 사용자의 웹 요청은 필터링 서버와 동시에 원래의 요청하고자 하는 서버에도 동시에 요청이 가기 때문에 효율성이 떨어지게 된다. 반면 본 논문에서 제시한 프록시를 이용한 필터링 시스템은 이러한 사용자와의 인터렉션이 훨씬 쉽고, 잠시 블록킹하거나 필터링 되어야 하는 요청에 대해서는 외부의 서버에게 패킷을 보내지 않을 수 있다는 장점이 있다.

3.2. 사용자 인증을 통한 필터링 알고리즘

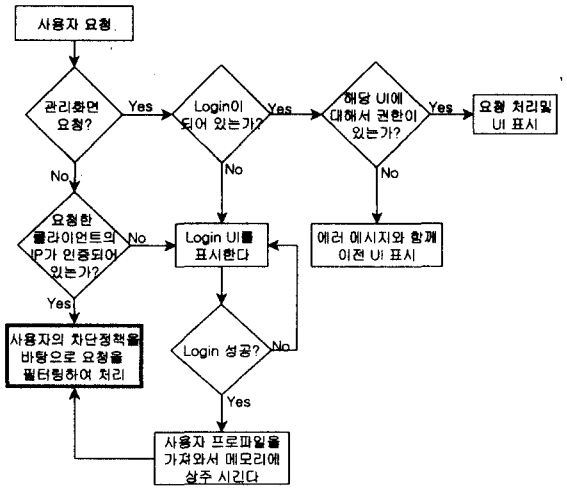
사용자는 '로그인' 이라는 과정을 통해서 인증을 거친 후에 사용자의 자신의 필터링 정책을 가지고 이후의 모든 웹 요청을 필터링 하게 된다. 이 절에서는 사용자 개인의 프로파일을 이용하여 어떻게 인증을 하고 이 인증을 통하여 필터링은 어떻게 되는지에 대한 자세한 알고리즘에 대해서 살펴볼 것이다.

사용자 인증을 하기 위해서는 관리 시스템과 이를 운영하기 위한 관영자가 필요하다. 이러한 관리 시스템은 필터링 서버 내부에 들어가 있으며 사용자 혹은 관리자와 필터링 시스템과의 인터페이스를 제공하여 준다.

사용자는 시스템 내에서 사용자 프로파일로 대표되며 사용자 프로파일에는 <사용자ID, 암호, 그룹명, 필터링 정책이름, 유휴 타임아웃 값>이 들어가게 된다. 필터링을

하는 대상으로는 사용자와 이 사용자들의 특성에 따라 묶은 그룹으로 구성된다. 그룹 또한 시스템 내에서 그룹 프로파일로 대표되며 그룹 프로파일에는 <그룹명, 필터링 정책이름, 기본 유휴 타임아웃 값>이 들어가게 된다. 사용자 프로파일과 그룹 프로파일에 있는 유휴 타임아웃 값은 사용자가 얼마의 시간동안 웹 요청을 하지 않으면 타임아웃이 발생되도록 하기 위한 값이다. 그리고 필터링 정책은 필터링 대상이 되는 URL들을 같은 특성을 가지고 있는 것끼리 묶어놓은 카테고리를 시간대로 스케줄링 해 놓은 것으로 어느 시간대에 어느 사이트를 막을 것인지에 대한 차단 규칙을 모아 놓은 것이다.

관리자는 사용자 프로파일 및 그룹 프로파일을 생성하거나 이들의 차단정책과 같은 설정을 생성, 변경할 수 있는 권한을 가지고 있다. 일반 사용자는 관리자에 의해 어떠한 그룹에 속하게 되며 필터링은 기본적으로 사용자가 속한 그룹의 필터링 정책을 따르게 되어 있다. 그러나 관리자는 특정그룹의 특정사용자만을 위한 필터링 정책을 만들고 변경하는 것 또한 가능하다.



[그림 4] 사용자 요청의 처리과정

[그림 4]은 사용자의 요청에 대해서 필터링 시스템의 처리과정을 간략히 나타낸 것이다. 사용자의 요청에 대해서 처음 하는 일은 이것이 외부의 웹 서버에 대한 요청인지 관리 화면에 대한 요청인지를 판단하는 것이다. 만약 외부 웹 서버에 대한 요청이라면 현재 요청한 클라이언트의 IP에 대해서 인증이 되어 있는지 살펴보고 인증된 경우에는 사용자의 차단정책을 바탕으로 요청을 필터링 하여 처리할 것이고, 그렇지 않다면 로그인 화면을 사용자에게 표시하여주고 로그인을 요청할 것이다. 사용자가 로그인을 하게되면 필터링 시스템은 사용자ID와 암호를 가지고 인증서버에 사용자 인증을 요청하게 된다. 사용자가 인증이 된 경우에는 사용자의 프로파일을 인증서버로부터 얻어와서 클라이언트의 IP와 매치 시켜 놓고, 이것을 통하여 이후의 모든 웹 요청에 대해는 인증된 것으로 해석한다. 로그아웃이 되는 경우는 다음의 두 가지 경우를 살펴 볼 수 있다. 첫 번째 방법은 사용자가 직접 관리화면에서 명시적으로 로그아웃을 하는 방법이고, 두 번째는 사용자 프로파일 데이터 중에서 유휴 타임아웃 값을 설정하여 일정시간동안 웹 요청을 하지 않으면 자동으로 로그아웃을 시키는 방법을 사용하는 것이다.

3.3 필터링 알고리즘

필터링 방법론은 이 논문의 범위에서 약간 벗어나는 것이므로 이 절에서 간단하게 살펴볼 것이다.

위에서 사용한 URL을 이용한 필터링은 TCP/IP 와 HTTP의 헤더에 있는 출발지와 목적지의 주소, 포트번호, 프로토콜 번호와 함께 호스트명(Hostname), 경로명(Pathname), 매개변수(Parameter), 쿼리(Query)를 모두 조합해서 필터링을 위한 URL을 생성하고 이것을 똑같은 방식으로 만들어진 DB와 비교를 수행함으로 필터링을 수행하게 된다. 이렇게 여러 개의 값을 조합해서 필터링을 수행함으로서 좀더 세밀하게 필터링을 할 수 있을 뿐만 아니라 가상호스팅(Virtual Hosting)과 같이 하나의 IP에 대해서 여러 개의 웹 Site가 있는 경우도 모두 구분해서 필터링이 가능하다.

4. 결론 및 향후 연구 과제

본 논문에서는 프록시를 이용한 필터링 시스템을 기본으로 사용자 인증 시스템을 통합하여 좀더 유연하고 확장성 있는 웹 필터링 시스템을 제안하였다. 이 시스템을 통해서 회사나 학교, 가정에서는 각 집단, 혹은 개인의 특성이나 상황에 따라서 다양한 필터링 정책을 사용하여 유해한 불법정보를 효율적으로 차단함과 동시에 네트워크 자원 또한 효율적으로 사용할 수 있을 것이다.

향후 연구 과제로서는 사용자인증을 RADIUS서버나 LDAP와 같은 표준 인증시스템과의 결합을 통해서 좀더 효율적이고 안정적인 인증 시스템을 만드는 것이다.

5. 참고문헌

[1] R. Fielding, J.Gettys, J.Mogul, H.Frystyk, L.Masinter, P.Leach and T.Berners-Lee, "Hypertext Transfer Protocol -- HTTP/1.1" RFC 2616, June 1999

[2] J. Postel, "Internet Control Message Protocol", RFC 792, September 1981

[3] M. Chatel, "Classical versus Transparent IP Proxies", RFC1919, March1996

[4] 김민수외 1인, "네트워크 트래픽 필터링 시스템의 설계 및 구현", 정보과학회지, 2000년 가을학술발표논문집(III), pp. 269~271