論文99-36S-8-1

LAN 모니터링을 통한 인터넷 유해 사이트의 사용자 접속 방지 시스템 개발

(Implementation of User Connection Prevention System through LAN Monitoring from Internet Harmful Site)

朴 亨 培 *, 鄭 重 壽 **

(Hyoung-Bae Park and Joong-Soo Chung)

요 약

오늘날 인터넷은 가장 주목받고 있는 정보통신의 산물로서 군림하고 있다. 특히, WWW은 GUI(Graphic User Interface) 인터페이스를 갖는 브라우저의 등장으로 인터넷의 발전에 가장 큰 공헌을 하였다. 초기 인터넷의 목적은 학문 연구의 수단이었으나 그 발전과 동시에 인터넷의 이용 방향은 학술, 경제, 문화 등 사회 각 분야로 넓혀지기 시작했다. 이와 같은 발전에 있어 가장 큰 역기능으로 나타난 것이 인명 경시, 인권 침해, 음란정보, 불건전 오락물등과 같은 유해 정보를 제공하는 호스트가 급속하게 늘고 있다는 것이다. 이와 같은 유해 정보의 급속한 증가는 초고속 정보화 사회에 힘입어 급속도로 추진되고 있으며, 초, 중등학교의 교육 현장에서는 범람하는 유해 정보에 대해 청소년을 보호할 수 있는 방안이 절실히 요구된다. 본 논문에서는 초, 중등학교의 LAN상에 통신되는 정보를 모니터링하면서 인터넷 유해 정보 사이트에 접속하는가를 점검하는데, 이때 인터넷 유해 정보 사이트에 접속하면, Hijacking기법을 도입하여 사용자가 접속하려는 호스트가 전송한 패킷인것처럼 가상적으로 재구성한 Fake Packet을 사용자에게 전달하여 인터넷 접속을 방해하는 시스템의 개발을 제시하였다. 또한 개발된 시스템을 안동대학교 LAN에 적용하여 인터넷 유해 사이트로 접속하는 사용자 정보를 모니터링한 결과, 인터넷 유해 사이트로의 접속금지에 대하여 만족한 성능을 수행하였다.

Abstract

The Internet is emerging as a powerful tool in the area of information and communication technology. The WWW has been especially contributed to increase the internet demand because of its browser which has "Graphic User Interface". Nowadays number of hosts that supply harmful information such as pornographic materials, and the infringement of human rights is rapidly increased. Access to such materials is very easy. Therefore security system which will protect young users from access to harmful host is needed. This paper presents implementation of user protecting system with LAN monitoring based on hijacking method over TCP/IP network. This system has database about harmful hosts at the Internet and monitors that the user traffic over LAN get touch with the hosts. The system can not make the user access the harmful host because it can decide whether the host requested by the user is harmful or not according to monitoring the traffic over LAN. The performance analysis on the developed system monitoring the traffic over LAN of Andong university is carried out. The performance analysis of monitoring results satisfies with preventing users from the connection to the internet harmful sites.

* 正會員, 情報通信大學院大學校 情報工學部 (ICU)

** 正會員, 安東大學校 電子情報産業學部 (Andong Nat'l Univ.)

※ 본 연구는 한국과학재단의 핵심전문연구과제(981-0918-097-2)의 지원으로 이루어진 연구결과입니다.

接受日字:1998年12月7日, 수정완료일:1999年5月3日

Ⅰ. 서 론

현대 사회는 급격한 산업화의 영향으로 청소년의 정서적, 신체적으로 유해한 환경이 사회 곳곳에 산재되어 있다. 이에 정부 및 각 사회 단체는 청소년에게 있어 유해한 환경의 배제를 통해 정서적으로나 신체적으로 건강한 사회 시민으로 만들기 위해 많은 노력을 하고 있다. 그러나 최근 인터넷이라는 매체가 갑자기 등장함으로 인해 청소년은 무방비인 상태에서 유해한 정보에 노출되게 되었다[2, 7].

이미 많은 초중등학교에 인터넷이 보급되기 시작했고 다수의 학생들이 인터넷을 사용하고 있 다[3]. 하지만 인터넷은 그 자신이 가지고 있는 특성상 그 어떤 기관도 내용에 관한 어떠한 제재력을 가지고 있지 않아서 인터넷에서 돌출되어 나오는 모든 정보는 여과없이 인터넷 사용자에게 곧바로 전달되게 된다[2, 4].

이러한 관점에서 보면 인터넷은 청소년의 정서 함양에 크게 악영향을 끼치는 요인이나 정보화사회로 가기 위해 반드시 청소년에게 교육되어야 할 내용이다. 현재 다수의 보안 시스템은 외부의 해커로부터 내부의 시스템을 보호하는 방화벽 시스템 구축에 주요한 목적이 있었다[8, 9]. 그러나 본 논문에서는 외부의 유해한 정보로부터 내부의 네트워 사용자를 보호하는 시스템이다.

그러므로 본 논문은 교육현장에 있어서 유해 사이트에 대한 등급을 정한 후 그 등급에 맞추어 학생들의 컴퓨터가 소속된 LAN 상의 정보흐름을 모니터링 한 후, hijacking 기법의 도입으로 유해 정보로부터 접속을 방지하는 시스템 개발을 소개하였다

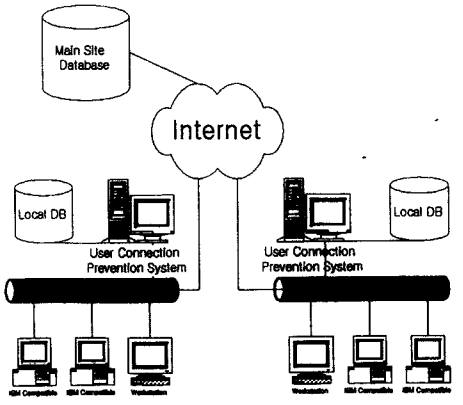

그림 1. 전체 시스템 구성도
Fig. 1. System Environment.

Ⅱ. 사용자 보호 시스템의 개요

본 논문에서 구현한 시스템의 적용 환경은 그림 1과 같다.개발된 시스템은 이더넷 LAN 상의 유해 정보 흐름을 모니터링하며, 중앙 유해 정보 사이트의 데이터 베이스는 인터넷을 통하여 각 초중등학교에 연결되고, 각 학교의 교사들에 의해 신고 및 등록된 유해 정보 사이트를 보유한다. 중앙의 유해 사이트 데이터 베이스는 주기적으로 초, 중등학교내 접속 방지시스템으로 전송된다. LAN 모니터링 기법을 도입한 hijacking 시스템이란 초, 중등학교내의 LAN에 접속된 학생들의 PC로부터 인터넷 유해 사이트에 접속을 감시하여 포착되면, 그 호스트로 페이크 패킷(Fake Packet)을 전송하여 TCP 접속을 종료시키는 hijacking 시스템이다.

본 논문에서 제시한 hijacking 시스템 개발은 현재의 모니터링 결과와 유해 사이트 등록을 위한 WWW(World Wide Web) 서비스 시스템으로 구성되며 각각의 시스템은 다음과 같이 동작한다.

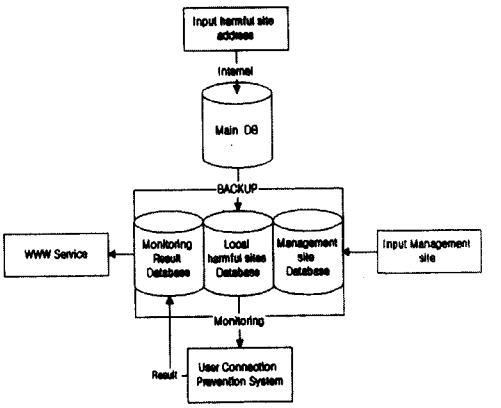

그림 2. 데이터 베이스 시스템의 구동 모형
Fig. 2. Database system architecture.

1. 유해 정보 사이트 데이터 베이스 시스템의 구축

본 논문에서 구현한 유해 정보 사이트 데이터 베이스 시스템의 구동 모형은 그림 2와 같으며, 관리자와 교사에 의해 등록된 유해 호스트는 WWW 인터페이스를 이용하여 중앙 데이터 베이스에서 저장되어진다. 중앙 데이터 베이스에 등록된 유해 호스트는 각 학교에 설치된 LAN 모니터링 시스템에 의해 주기적으로 로컬(Local) 데이터 베이스로 백업을 받게 한다. 그림 3은 유해 호스트를 중앙 데이터 베이스로 등록하는 화

면이다. 이 때 등록될 유해 호스트는 도메인 네임과 IP 주소의 2가지중 하나로 등록이 되어 진다. 그러나 LAN 모니터링중 데이터 베이스 검색시에 사용되는 것은 IP 주소이므로 도메인 네임으로 등록시에는 IP 주소로 변환해 주어야 한다.

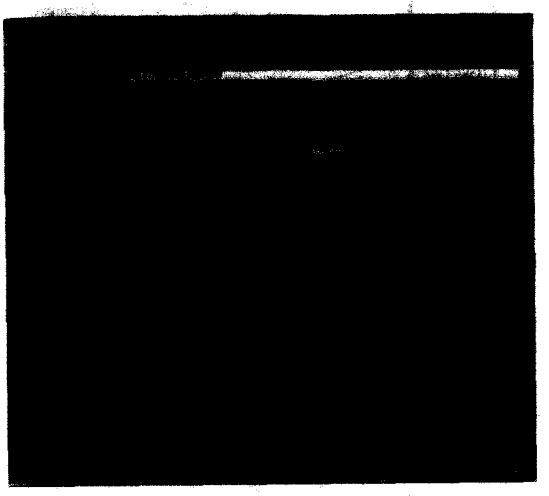

그림 3. 유해 호스트 등록 WWW인터페이스
Fig. 3. WWW interface for harmful site registration.

2. LAN 모니터링 시스템의 구축

본 시스템은 GCC 7.2 컴파일러와 System independent Packet Capture Library인 libpcap 0.4a2버전을 사용하여 구축하였다.

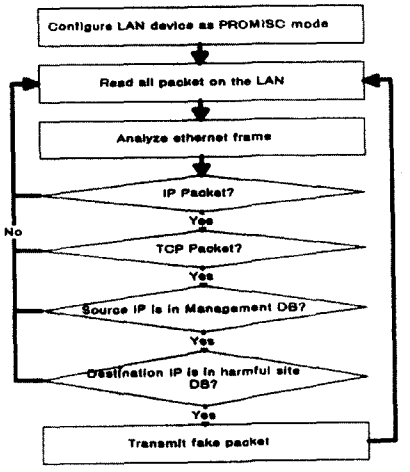

그림 4. LAN 모니터링 시스템의 동작 원리
Fig. 4. Operation of monitoring system.

LAN 모니터링 시스템이 동작하는 원리는 그림 4와 같다.

LAN 모니터링은 이더넷의 통신방법을 이용한 프로그램이다. 이더넷상에서 두 호스트간에 통신을 하려면 호스트간에 연결을 맺어 놓고 패킷을 전송하는 것이 아니라 보내고자 하는 패킷 자체를 이더넷상에 브로드캐스트하게 된다.

이 때 각각의 호스트는 자신에게 오는 패킷만을 읽을수 있다. 하지만 네트웍 디바이스를 "promiscuous mode"로 열면 네트웍상에 지나가는 모든 패킷을 다 읽어 오게 된다. 본 시스템은 이 원리를 이용해서 다음과 같은 단계로 구현했다.

1) 시스템은 우선 설치된 네트웍 디바이스를 찾아 디바이스를 연다 [그림 5] .

```
void OpenDevice() {
// Find LAN device
        name = pcap_lookupdev(errbuf);
        if(name==NULL) { printf("Failed\n");}
    // Open the device and assign it to device open
    // descriptor p
        p = pcap_open_live(name,1600,1,1000,errbuf);
}
```

그림 5. Network device open 절차
Fig. 5. Network device open procedure.

2) 열려진 디바이스에서 읽어들일 패킷의 종류를 결정하는 소스는 그림 6과 같다.

```
pcap_lookupnet(name,&localnet,&netmask,errbuf);
// set the protocol type of packet.
if((pcap_compile(p,&prog,"tcp",1,netmask))<0) {
  printf("%s",pcap_geterr(p));
  return;
}
pcap_setfilter(p,&prog);
```

그림 6. Network Device로부터 읽어 들일 Protocol 설정
Fig. 6. Set the protocol type to read from network device.

3) TCP 연결설정을 종료시켜야 함으로 실제 읽어들일 데이터는 TCP 패킷만으로 설정하고 그림 7과 같이 네트웍 디바이스로부터 데이터를 읽어들인다.

```
do {
// Pass the TCP packet pointer via structure hdr
  data = pcap_next(p,&hdr);
```

```
  for(i=0; i< hdr.bh_caplen;i++){
// Parse the hdr structure
    ParsePacket((unsigned char)data[i]);

  }
// Analyze TCP packet
  if( CheckHarmSite() == TRUE) {
  // If harmful site, send FIN packet
    SendFakePacket();
  }
}while(1);
```

그림 7. Network device로부터 TCP/IP packet capture
Fig. 7. TCP/IP packet capturing from network device.

네트웍 디바이스에서 읽어들인 데이터는 IP 헤더 구조체에서 송신지 IP 주소와 수신지 IP 주소를 분석하여 유해 호스트에 접속하고 있으면 TCP 제어 플래그의 종료(FIN) 비트를 '1'로 설정하여 송신지 IP 주소인 시스템으로 전송하여 강제로 TCP 접속을 해제시킨다.

3. Hijacking 시스템의 구축

본 시스템은 클라이언트의 OS에 구애받지 않고 단순히 페이크 패킷 전송만을 통해서 TCP 연결을 종료시키는 방식과 그 현황을 모니터링하는 방식을 선택하여 구축하였다.

페이크 패킷 전송 시스템의 구동 원리는 그림 8과 같으며,관리영역의 PC가 유해 호스트에 TCP 연결을 설정을 요구하고 유해 호스트로부터 TCP 연결 설정 응답이 PC에게 송신 될 때 모니터링 시스템은 TCP의 응답번호와 순서번호를 설정하고 TCP 제어 플래그의 종료 비트를 '1'로 설정하여 페이크 패킷을 송신한다. 이 때 설정되는 응답번호의 값은 유해 호스트에서 PC로 전송한 값과 동일하고 순서번호의 값은 유해 호스트에서 PC로 전송한 값에 TCP 전송 패킷의 데이터 영역의 길이를 더한 값과 같다.

만약, 유해 호스트에서 PC에게 TCP 연결을 설정(SYN비트를 '1'로 설정)하는 단계이면, 데이터 영역의 길이는 0이 된다. 재구성된 패킷은 그림 9와 같이 Sendto 함수를 이용하여 목적지 호스트로 전송한다. 따라서 재구성되어 전송된 패킷은 목적지 호스트인 PC로 전송이 되어 TCP 연결을 종료시킨다.

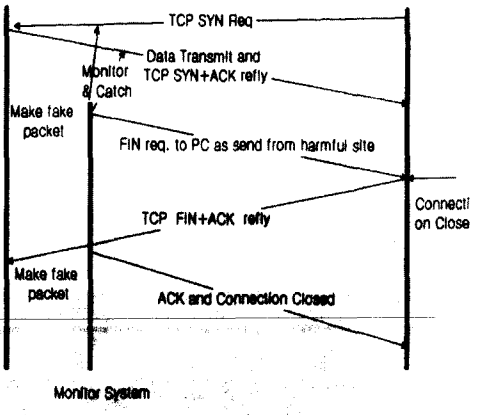

그림 8. Hijacking system의 구동 원리
Fig. 8. Operation scenario of hijacking system.

```
void SendPacket(struct sp_RemakePacket *sp)
{
 int sp_fd;
 struct sockaddr_in sp_server;
 // Setup protocol and open the socket
if((sp_fd=socket(AF_INET,SOCK_RAW,IPPROTO_RAW))
   == -1) { perror("Couldn't open Socket!!"); exit(1); }
 // Construction of destination
bzero((char *)&sp_server, sizeof(struct sockaddr));
sp_server.sin_family = AF_INET;
sp_server.sin_addr.s_addr == IP_DEST;
 // Send sp->buffer's contents to IP_DEST using
 // connectionless system call.
  sendto(sp_fd, (char *)(sp->buffer), sp->datalen, 0,
  (struct sockaddr *)&sp_server,sizeof(struct sockaddr));
  }
```

그림 9. Fake packet 전송
Fig. 9. Transmit fake packet.

4. WWW 서비스 시스템의 구축

구현된 시스템에서 WWW 서비스는 크게 호스트 등록 서비스와 LAN 모니터링된 결과 서비스로 구성되어진다. 호스트 등록 서비스는 유해 호스트 등록 서비스와 관리 호스트 등록 서비스로 구성되어진다 [그림 3]. LAN 모니터링 결과 서비스는 그림 10에서 같이 지역 데이터 베이스에서 유해 사이트에 접속한 호스트의 Alias와 IP 주소를 가져와서 WWW 브라우저에 출력해준다.

시스템은 학교내 어디서든 관리자가 항상 모니터링 결과를 확인하고 인터넷 사용을 지도할 수 있게 하며,

인터넷이 연결된 어느 곳에서든 유해 호스트를 등록하면 전체 지역 데이터 베이스에 동일하게 전송된다.

```
#include <stdio.h>
#include "msql.h"
#define DBFILENAME "DB_URL"

void main(int argc, char *argv[]) {
        register int x,m=0;
        m_result *result;
        int sock,i,j=0,count=0;
        char *cl;

        printf("Content-type: text/html%c%c",10,10);
        getenv("REQUEST_METHOD"),"GET");
        sock = msqlConnect(NULL);
        msqlSelectDB(sock,DBFILENAME);
        sprintf(Sql,"SELECT * FROM tblLanMonitor
                where Flag = 'Y'");
        msqlQuery(sock,Sql);
        result = msqlStoreResult();
        // Display result to web browser
        for (i=0;i<result->numRows;i++) {
           printf("%s(%s)\n",result->queryData->data[0],
                        result->queryData->data[2]);
           // Move next record
           result->queryData = result->queryData->next;
        }
        msqlFreeResult(result);
        msqlClose(sock);
}
```

그림 10. LAN 모니터 결과 출력
Fig. 10. Output procedure for LAN monitoring result.

Ⅲ. 시험환경 및 기대효과

인터넷을 사용하고 있는 국립 안동대학교 1,2학년 학생 50명을 대상으로 한 설문 조사에 따르면, 50명 중 31명이 인터넷을 통해 음란물을 접해 보았다고 했으며, 31명 중 28명이 WWW을 통해 음란물을 접하며 인터넷의 음란물의 접속도 아주 쉽다고 했다. 따라서 인터넷상의 유해 정보에 대한 통제가 이루어져야 한다.

본 시스템의 시험 환경은 국립 안동대학교의 LAN 환경으로 100Mbps의 FDDI 백본망에 10Mbps급 이더넷을 서브넷으로 인터넷망과의 접속은 T1으로 구축된다. 따라서 10Mbps급 이더넷 LAN환경에서 12대의 클라이언트와 본 논문에서 개발된 시스템을 접속하여 시험하였다. 구현된 시스템은 Pentium 120Mhz, RAM 8MB의 시스템에 Redhat Linux 4.2으로 설치하였다.

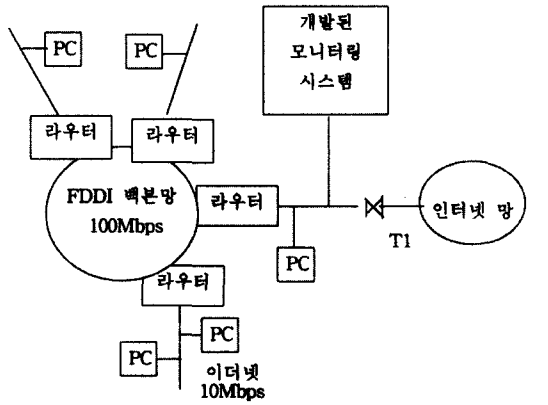

그림 11. 안동대학교 LAN환경과 개발된 시스템의 시험환경
Fig. 11. Target system test environment based on Andong National Univ. LAN.

본 시스템을 구축 및 설치한 후의 기대되는 효과는 다음과 같다.

- 학교내 네트웍상에서 학생들이 유해 사이트에 접속하는 것을 방지할 수 있다.
- 설치에 필요한 시스템이 적고 설치가 쉽다.
- 관리자 및 교사에 의해 교육적으로 유해한 사이트의 구분이 가능해진다.
- Telnet, WWW, FTP등 인터넷상의 서비스에 대해 호스트상의 접속은 방지할 수 있다.

Ⅳ. 유해 방지 시스템의 성능해석

인터넷에 접속하는 정보를 모니터링한 유해방지 시스템개발중 성능에 영향을 미치는 이더넷 정보 흐름의 모니터링 기법에 대해 살펴보았다. 본 시스템에서 하드웨어로부터 수신되는 이더넷 프로토콜 정보를 개발된 시스템에서 분석하여 인터넷의 유해 정보 사이트에 접속한다는 사실을 알고서 페이크 패킷을 송출하기 까지의 소요시간은 다음과 같다.

- 펌웨어 소요시간: 1ms
- 펌웨어에서 소프트웨어 프리미티브 호출 처리시간: 0.3ms
- 모니터링 소프트웨어 처리시간: 0.2ms
- 페이크 패킷을 송출 까지의 소요시간: 0.1ms

위의 사실로 보아 한 개의 이더넷 프로토콜 정보를 확인하여 페이크 패킷 송출시간 까지의 전체 소요시간은 1.6ms이다. 안동대학교 LAN의 서브넷인 이더넷을 대상으로 시험했을 때, 그 전송속도는 10Mbps이므로 가장 짧은 TCP/IP 패킷의 경우 최소 64바이트 이므로 이러한 프레임의 트래픽이 이더넷 미디움의 약 20%를 차지하면, 초당 약 8,000개가 전달된다. 또 개발된 시스템에서 이더넷 프로토콜 정보를 확인하여 페이크 패킷 송출시간 까지의 전체 소요시간은 1.6ms이므로 현재의 개발된 시스템은 초당 약 650개의 이더넷 프레임을 모니터링할 수 있다. 따라서 이더넷의 트래픽중 약 8%(8,000/650)의 정보를 모니터링 한다는 결론을 얻는다. 이는 현재 HP 프로토콜 분석기가 이더넷 LAN 통신 환경하에서 수신한 TCP/IP 프레임 개수를 분석한 결과와 유사함을 알 수 있다[10].

이와 같은 상황에서 사용자가 인터넷 유해 사이트의 접속시 TCP 접속을 위해 3개의 패킷을 송, 수신한후 7개의 TCP/IP 패킷을 추가로 송, 수신할 경우, 개발된 시스템으로 TCP/IP 패킷을 모니터링하면 수적지 IP 주소가 데이터 베이스에 등록된 인터넷 유해 사이트인지 파악 가능하다. 따라서 사용자가 7개의 TCP/IP 데이터 전달 패킷을 인터넷 유해 사이트와 추가로 송, 수신시에는 개발된 시스템에서 페이크 패킷을 전달하여 TCP 접속을 해제 한다는 결론을 내릴 수 있다. 이와 같은 결론으로 미루어 보아 현재의 개발된 시스템으로 10Mbps의 이더넷 LAN 사용자들의 인터넷 유해 사이트 접속을 충분히 막을 수 있다.

V. 결 론

현재 인터넷상에서 유해한 정보의 범람은 청소년 보호와 인터넷 교육이라는 두 가지 상반된 문제를 야기시키고 있으며, 이 두 문제를 해결하고 청소년에게 인터넷을 빨리 학습하게 하여서 건전하고 바른 방향으로 지도하기 위해서는 인터넷 사이트들에 대한 등급화와 각 등급에 따른 접속 제한을 두는 것이 무엇보다 시급하다.

이미 사용자의 PC에 접속 제한 프로그램을 설치하는 방안이 개발되었으나 그것은 사용자가 그 프로그램을 삭제하거나 설치하지 않으면 제재할 수 없다. 그러므로 인터넷 접속 제안의 보다 올바른 방법은 네트웍 자체에 접근 제한을 두는 것이다. 그럼으로 본 논문에서 개발한 시스템은 청소년들이 학교내에서 인터넷을 통해 유해 사이트로 접근하는 것을 막아 줄 것이다. 또한 개발된 시스템 성능도 분석하였는데 현재 개발된 시스템의 한 개의 이더넷 프로토콜 정보를 확인하여 페이크 패킷 송출시간 까지의 전체 소요시간은 1.6ms로서 이더넷과 같은 10Mbps의 미디움에서 모니터링을 수행하여 인터넷 유해 사이트 접속을 충분히 막을 수 있음을 입증하였다.

본 논문에 이어 연구되어야 할 분야는 가정에서 모뎀을 통해 접속하는 사용자의 유해 호스트 접근 제어와 유즈넷 접근에 있어 뉴스 그룹별 접근 제어이다. 또 개발된 시스템의 성능을 향상시켜 10Mbps 이상의 고속의 통신망에서도 인터넷 접속을 막을 수 있도록 계속적인 보완 개발이 요구된다.

참 고 문 헌

[1] 한국전산원 보안기술표준팀 홈페이지, http://security.nca.or.kr/

[2] 이사범, "인터넷 정보보호 대책에 관한 연구", 월간「정보화 사회」,1997. 4월호, pp. 46~49

[3] 윤준수, "멀티미디어로서 인터넷의 등장과 토탈 패러다임으로의 진화", 한국언론학회 1996년 추계 정기학술대회 발표 논문

[4] 정인성, "하이퍼미디어와 컴퓨터교육의 미래",「교육공학연구」제6권 제1호 별책, 1990. 12,

[5] Sniffit, "http : // reptile.rug.ac.be/~coder/sniffit/sniffit.html"

[6] Synlog, "http : // www.whitefang.com/synlog.html"

[7] 정보통신윤리위원회, "http : // www.icec.or.kr/"

[8] 필주, "초고속 정보통신망과 인터넷의 접속에 따른 통신망 보안", 통신정보보호학회지, 제5권 4호, 1995년 12월호

[9] 임채옥, "인터넷 방화벽시스템의 구축방법과 연구 개발", 통신정보보호학회지, 제4권 3호, 1994년 9월호

[10] "HP Internet Advisor Spec.", 1996.

저 자 소 개

朴 亨 培(正會員)

1997년 2월 안동대학교 컴퓨터공학과 (학사). 1998년 3월 ~ 현재 정보통신대학원대학교 정보공학부 석사과정 재학

鄭 重 熹(正會員)

1981년 2월 영남대학교 전자공학과 (학사). 1983년2월 연세대학교 전자공학과 (석사). 1993년 8월 연세대학교 전자공학과 (박사). 1983년 3월 ~ 1994년 2월 ETRI 연구원, 선임연구원. 1987년 8월 ~ 1989년 8월 벨지움 Alcal/Bell Telephone사 객원연구원. 1994년 3월 ~ 현재 국립 안동대학교 공과대학 전자정보산업학부 조교수