SNMP를 이용한 트래픽 폭주 공격 검출

Detection of Traffic Flooding Attack using SNMP

김선영
충북대학교 컴퓨터공학과

박원주
한국전자통신연구원 정보보호연구본부

유대성
충북대학교 컴퓨터공학과

서동일
한국전자통신연구원 정보보호연구본부

오창석
충북대학교 전기전자컴퓨터공학부

Sun-Young Kim (sykim@nwork.chungbuk.ac.kr)
Dept. of Computer Engineering, Chungbuk National University

Won-ju Park (wjpark@etri.re.kr)
Information Security Technology Division, ETRI

Dae-Sung Yoo (dsyoo@nwork.chungbuk.ac.kr)
Dept. of Computer Engineering, Chungbuk National University

Dong-Il Seo (bluesea@etri.re.kr)
Information Security Technology Division, ETRI

Chang-Suk Oh (csoh@nwork.chungbuk.ac.kr)
School of Electrical and Computer Engineering, Chungbuk National University

중심어 : SNMP, MIB, 트래픽 폭주 공격

Keyword : SNMP, MIB, Traffic Flooding Attack

요 약

최근 다양한 트래픽 폭주 공격으로 인해 원격 호스트나 해당 네트워크가 정상적인 서비스를 제공할 수 없는 사례가 빈번히 발생하고 있다. 이러한 공격은 다른 해킹을 위한 초석으로 사용될 수 있어 공격 기법 중 가장 위험한 공격으로 분류되고 있다. 본 연구에서는 이러한 트래픽 폭주 공격을 검출하기 위해 SNMP의 MIB를 이용해 시스템의 트래픽 정보를 수집한다. 대부분의 트래픽 폭주 공격들은 유사한 트래픽 특징을 보이므로 이러한 특징을 이용하여 임계값을 적용시켜 분석하였다. 그 결과, 각각의 트래픽 폭주 공격의 유형에 따라서 독특한 특성을 가짐을 발견하였다. 본 연구의 결과로 얻어진 이러한 특징들을 트래픽 폭주 공격을 조기에 탐지 하는 기법과 보호하는 기법 연구에 많은 도움을 줄 것으로 예상된다.

Abstract

Recently it frequently occur that remote host or network device breaks down because of various traffic flooding attacks. This kind of attack is classified an one of the most serious attacks of it can be used to a need of other hackings. This research is gathering system's informations for detecting a traffic flooding attack using the SNMP MIB. We analyze the traffic characteristic applying the critical value commonly used in analytical procedure of traffic flooding attacks. As a result of this analysis, traffic flooding attacks have a special character of its own. The proposed algorithm in this paper would be more available to a previous detecting method and a previous protecting method.

I. 서론

초기의 해커들은 단순히 시스템의 버그를 이용하여 루트 권한을 얻는 형태였지만, 최근 해커들은 루트 권한을 얻는 목적 이외에도 네트워크에 트래픽을 증가시켜 정상적인 서비스를 제공할 수 없는 DoS 공격 형태로 많이 나타나고 있다. 이러한 공격의 피해 사례는 Yahoo, eBay등 많은 전자상거래를 제공하는 사이트들을 예로 들 수 있다. 또한 최근 대표적인 공격 피해 사례는 "1.25 인터넷 대란"이라 말하는 SQL slammer 웜 공격이 바로 대표적이라 할 수 있다. 이렇듯 인터넷에 개방되어 있는 시스템들이 트래픽 폭주 공격에 매우 취약함을 보여 주고 있다. 이러한 트래픽 폭주 공격의 피해가 심각하게 여겨지고 있으며, 이에 대한 다양한 연구가 진행되

* 본 연구는 한국전자통신연구원 연구과제로 수행 되었습니다.
접수번호 : #031115-002
접수일자 : 2003년 11월 15일, 심사완료일 : 2003년 12월 2일

*교신저자 : 김선영, e-mail : sykim@nwork.chungbuk.ac.kr

고 있다. 기존의 트래픽 폭주 공격을 검출하는 방법은 침입 탐지 시스템을 이용하여 네트워크상의 모든 패킷을 캡쳐하여 패킷 헤더를 분석하는 방법이다[1]. 이러한 방법은 모든 패킷을 수집함으로써 트래픽을 분석하므로 시스템 자체의 많은 과부하로 인하여 정상적인 검출을 할 수 없다 또한 이러한 검출 방법은 기존에 정의된 공격만을 탐지하기 때문에 새로운 트래픽 폭주 공격은 탐지할 수 없는 문제점을 가지고 있다. 이러한 문제점을 고려하여 본 논문에서는 트래픽 폭주 공격을 분석하였고, 분석된 공격의 특징을 추출하여 적용하였다. 또한 SNMP(Simple Network Management Protocol)를 이용하여 트래픽 폭주 공격을 검출함으로써 시스템의 과부하 문제를 해결하였고, 공격의 특징을 이용함으로써 새로운 유형의 트래픽 폭주 공격에 대해서도 효과적으로 탐지하였다[2].

II. SNMP를 이용한 트래픽 폭주 공격 검출

기존의 트래픽 폭주 공격에 대한 탐지 방법은 대부분이 침입 탐지 시스템을 이용한 탐지였다. 이러한 침입 탐지를 이용한 방법은 트래픽 폭주 공격을 탐지하기 위해 네트워크상의 모든 트래픽을 캡쳐하여 패킷 헤더 정보를 분석함으로써 많은 시스템 부하와 정확한 트래픽 폭주 공격을 탐지 할 수 없었다[3]. 또한 침입탐지 시스템의 침입 규칙 데이터에 없는 공격의 경우에는 검출할 수 없었다. 따라서 이러한 문제를 해결하기 위해 이 장에서는 좀 더 효율적이고, 현실에 적용 가능한 방법인 SNMP를 이용한 트래픽 폭주 공격 검출 알고리즘을 제안하고 구현하였다.

1. 공격 탐지

네트워크 상에서 트래픽이 발생하게 되면 트래픽 수집 방법으로 SNMP를 이용하여 트래픽을 수집하게 된다. SNMP MIB(Management Information Base) 객체중 관심 대상의 트래픽에 대하여 선별적인 수집을 하게 되며, 수집된 트래픽을 수치적으로 변환하기 위해서 MRTG(Multi Router Traffic Grapher)를 이용하여 로그값을 생성하게 된다[4],[5],[6]. 수집된 각 MIB 객체의 정보는 프로토콜별 트래픽 분석 단계로 전달되어 지며 전달된 값들은 분석 단계에서 공격 트래픽과 정상 트래픽에 대한 판별 데이터로 쓰이게 된다. 이러한 데이터는 트래픽 분석 단계를 통해서 최종적으로 관리자에게 현재 네트워크 상의 트래픽에 대한 전체적인 분석을 통보하게 된다[7]. SNMP를 이용한 트래픽 폭주 공격 탐지 방법은 다음과 같고 그림 1은 SNMP를 이용한 트래픽 분석의 흐름도를 나타내고 있다.

(1) 트래픽 발생
(2) SNMP 프로토콜을 이용하여 트래픽 수집
(3) 수집된 트래픽에 대하여 프로토콜별 MIB 객체 정보를 통하여 정상 트래픽과 공격 트래픽에 대한 분석
○ 공격을 검출하는 MIB 객체의 트래픽 발생 유무 검사
○ 발생된 트래픽 크기의 변화량 검사
(4) 수집된 트래픽 판정

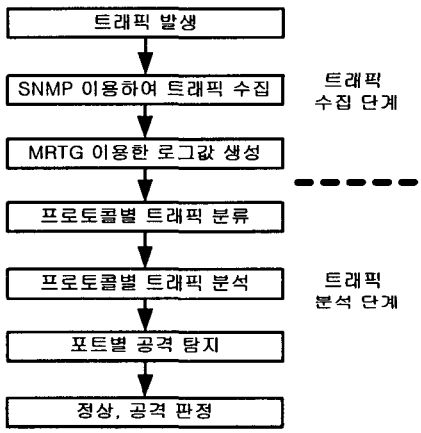


그림 1. SNMP를 이용한 트래픽 분석의 흐름도

트래픽 분석에 사용되는 MIB 객체는 각 프로토콜별로 실험을 통해 얻어진 데이터를 분석하여 정상 트래픽과 공격 트래픽을 구분할 수 있는 MIB 객체를 선택하였다. 표 1은 제안된 알고리즘에 사용된 MIB 객체를 나타낸다[8].

표 1. 제안된 알고리즘에 사용된 MIB 객체

프로토콜	MIB 객체
IP	ipInReceives
TCP	tcpInSegs
	tcpInErrs
ICMP	icmpInMsgs
	icmpOutMsgs
	icmpInEchos
	icmpOutEchoReps
UDP	udpInDatagrams
	udpOutDatagrams
	udpNoPorts
	udpInErrors

표 1에서 선정된 MIB값을 기본으로 하여 프로토콜별로 트래픽을 분해한 후 입출력되는 트래픽에 대해서 그 특징을 분석하게 된다. 트래픽 분석에 사용되는 기본 알고리즘은 공격 트래픽이 발생되었을 경우, 트래픽의 특징을 분류하여 탐지하게 된다. 공격이 발생되었을 경우, 트래픽의 특징은 해당 포트에서의 MIB 객체 중 공격에 반응하는 특정한 MIB 객체가 존재한다는 것과 공격에 반응하는 MIB 객체의 트래픽 크기가 일정한 범위안에서 일정한 크기를 유지한다는 것이다. 이 두가지 특성을 이용하여 프로토콜 별로 트래픽을 분석하여 관리자에게 트래픽 분석 내용을 통보하게 된다. 본 연구과제에서 제안한 SNMP를 이용한 트래픽 폭주 공격 검출 알고리즘의 구현은 트래픽 수집 모듈과 트래픽 분석 모듈로 구성되어 진다. 트래픽 검출 알고리즘은 TCP 트래픽 검출 알고리즘, ICMP 트래픽 검출 알고리즘 그리고 UDP 트래픽 검출 알고리즘으로 세분화되어 진다.

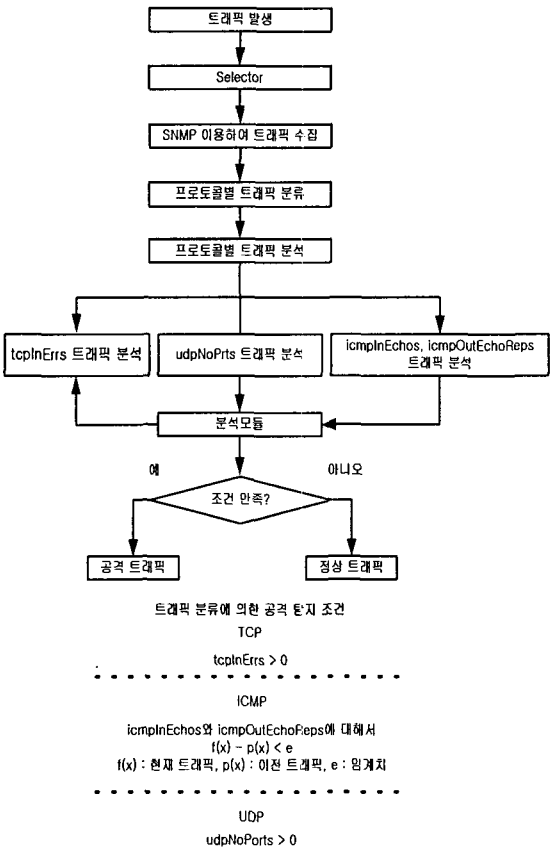


그림 2. 트래픽 수집 및 검출 알고리즘

그림 2는 SNMP를 이용한 트래픽 폭주 공격 검출 알고리즘의 구성도를 도시하였다. 구성도에서 보는 바와 같이 일정 시간마다 트래픽 수집 모듈을 통해 각 시스템의 트래픽 정보를 SNMP 폴링을 통해 가져오게 된다. 이러한 폴링을 통해서 지정된 MIB 객체 ipInReceives, tcpInSegs, tcpInErrs, udpNoPorts, icmpInEchos, icmpOutEchoReps를 가져와 MRTG를 이용하여 정형화된 로그값을 생성한다. 이렇게 생성된 로그값은 트래픽 분석 모듈을 통해 각각의 프로토콜 별로 분해하게 되는 과정을 도시하였다.

2. 트래픽 폭주 공격 검출 알고리즘

트래픽 폭주 공격을 탐지하기 위하여 SNMP MIB 객체에 의해 수집된 전체 트래픽중 공격과 밀접한 반응을 보이는 MIB 객체를 선정하여 수집하게 된다. 수집된 MIB객체의 트래픽 데이터는 각 프로토콜별 분석 모듈에서 정상 트래픽과 공격 트래픽을 분석하게 된다.

2.1. TCP 트래픽 분석 알고리즘

TCP 트래픽 검출 알고리즘은 수신된 IP 데이터그램에 대한 트래픽 중에서 SNMP MIB 객체중 tcpInSegs와 tcpInErrs에 대응되는 트래픽을 수집하여 분석하여 정상 트래픽 유무를 판단한다. 그림 3은 TCP 트래픽 분석 알고리즘을 도시하였다.

```
Traffic analysis procedure of TCP
  let Log() be a reading a log's value
  let ε be a threshold
  let f(x) = T(curr) : current log value
  let p(x) = T(prev) : previous log value
  let T be a table for storing
  let attack() be a attack traffic alarm
  let innocence() be a innocence
   traffic alarm
     if tcpInSegs > 0 then
        call tcp traffic analysis function
        if tcpInErrs > 0 then
           T_in(curr) <- Log(tcpInErrs_curr)
           T_in(prev) <- Log(tcpInErrs_prev)
           if f(x) - p(x) < ε
              return attack(T_in(curr))
           else
              return innocence(tcpInSegs)
        else
           return innocence(tcpInSegs)
     else
       pass tcp traffic analysis function
```

그림 3. TCP 트래픽 검출 알고리즘

알고리즘의 처리과정을 보면 전체 수신된 IP 데이터그램의 트래픽 중에서 tcpInSegs에 해당하는 트래픽이 발생하게 되면 TCP 공격 검출 함수를 호출하게 되며 호출된 함수에서는 TCP를 이용한 공격의 특징인 tcpInErrs MIB 객체에 대응되는 트래픽이 발생하는지 검사하게 된다. tcpInErrs에 대응되는 트래픽의 발생이 없다면 현재 발생된 TCP 응용 프로그램에 대한 트래픽에 대해서 정상적인 트래픽임을 관리자에게 통보하게 된다. 하지만 tcpInErrs에 대응되는 트래픽이 발생하게 된다면 발생된 tcpInErrs 트래픽을 테이블에 저장한 후 다음 발생된 tcpInErrs 트래픽과 오차 ε을 계산하게 된다. 계산된 오차가 임계치 안에 존재한다면 관리자에게 공격을 통보하게 되고 그 반대는 정상 트래픽으로 관리자에게 통보된다.

2.2. UDP 트래픽 분석 알고리즘

UDP 트래픽 검출 알고리즘에서는 UDP MIB 객체중 udpNoPorts에 해당하는 트래픽이 발생하는지를 검사하게 된다. 그림 4는 UDP 트래픽 분석 알고리즘의 처리과정을 나타낸다.

```
Traffic analysis procedure of UDP
  let Log() be a reading a log's value
  let ε be a threshold
  let f(x) = T(curr) :
            current log value
  let p(x) = T(prev) :
              previous log value
  let T be a table for storing
  let attack() be a attack
  traffic alarm
  let innocence() be a
   innocence traffic alarm
     if udpNoports > 0
        call udp traffic
         analysis function
        T_in(curr) <- Log(udpNoPorts_curr)
        T_in(prev) <- Log(udpNoPorts_prev)
        if f(x) - p(x) < ε
           return attack(T_in(curr))
        else
           innocence ()
     else
        pass udp traffic analysis function
```

그림 4. UDP 트래픽 검출 알고리즘

UDP 응용 프로그램을 사용하는 트래픽이 발생될 경우 공격 트래픽이라면 상위 응용 서비스로 전달되지 못하고, 수신된 트래픽에 대해서 udpNoPorts MIB 객체에 대응되는 트래픽으로 모두 발생하게 된다. 이때 발생된 트래픽을 테이블화하여 현재의 입력값과 그 전 시간의 입력값을 근사 다항식에 적용시켜 오차를 구하게 된다. 이때 생성된 오차는 임계값과의 비교를 통하여 오차가 임계값안에 있을 경우 공격으로 탐지하게 된다. 탐지된 입력 트래픽은 관리자에게 공격 트래픽이 UDP 프로토콜을 사용하여 발생되고 있음을 통지하게 된다.

2.3. ICMP 트래픽 분석 알고리즘

ICMP 트래픽 검출 알고리즘에서는 임계값을 적용하여 공격을 검출하게 된다. 우선 ICMP 트래픽이 발생하게 되면 icmpInEchos와 icmpOutEchoReps에 대응되는 트래픽을 테이블에 저장하게 된다. 다음 시간대에 발생된 icmpInEchos와 icmpOitEchoReps의 트래픽을 다시 테이블에 저장하게 되며 그 전에 저장된 값과의 트래픽 변화량을 계산하게 된다. 일반적으로 공격 트래픽의 경우에는 트래픽 변화량이 ε에 근사해지므로 현재의 트래픽 값과 이전 시간의 트래픽 값을 통하여 근사 다항식을 생성하게 된다. 생성된 근사 다항식을 통하여 ε의 값을 구한 후 ε이 임계치에 만족하게 되면 관리자에게 공격임을 통보하게 된다. 그림 5는 ICMP 트래픽 분석 알고리즘의 처리과정을 보여준다.

```
Traffic analysis procedure of ICMP
  let Log() be a reading a log's value
  let ε be a threshold
  let f(x) = T(curr) : current log value
  let p(x) = T(prev) : previous log value
  let T be a table for storing
  let attack() be a attack traffic alarm
  let innocence() be a innocence traffic alarm
     if icmpInEchos > 0
              and icmpOutEchoReps then
        call icmp traffic analysis function
        T_in(curr) <- Log(icmpInEchos_curr)
        T_out(curr) <- Log(icmpOutEchoReps_curr)
        T_in(prev) <- Log(icmpInEchos_prev)
        T_out(prev) <- Log(icmpOutEchoReps_prev)
        if f(x) - p(x) < ε
           return attack(T_in(curr))
        else
           return innocence()
     return
       pass icmp traffic analysis function
```

그림 5. ICMP 트래픽 검출 알고리즘

III. 실험 및 고찰

트래픽 분석 알고리즘에서 사용될 임계값을 구하기 위하여 TCP SYN Flooding, ICMP Flooding, UDP Flooding 공격을 실시하여 임계값 변화에 공격 트래픽 탐지율을 구하고, 여기서 구해진 임계값을 토대로 알고리즘에 적용하게 된다.

표 2. 임계값 변화에 따른 TCP 공격 탐지율

임계치 (ε)	공격 트래픽량	공격으로 탐지된 트래픽량	정상으로 처리된 공격트래픽량	탐지율 (%)
0	6823	3417	3406	50.08
1	6823	4390	2433	64.34
2	6823	4878	1945	71.49
3	6823	5849	974	85.72
4	6823	6823	0	100
5	6823	6823	0	100

표 3. 임계값 변화에 따른 UDP 공격 탐지율

임계치 (ε)	공격 트래픽량	공격으로 탐지된 트래픽량	정상으로 처리된 공격트래픽량	탐지율 (%)
0	22920	6549	16371	28.57
1	22920	16372	6548	71.43
2	22920	22920	0	100
3	22920	22920	0	100

표 4. 임계값 변화에 따른 ICMP 공격 탐지율

임계치 (ε)	공격트래픽량	공격으로 탐지된 트래픽량	정상으로 처리된 공격트래픽량	탐지율 (%)
0	12413	885	11528	7.13
1	12413	3546	8867	28.57
2	12413	6207	6206	50.00
3	12413	8865	3548	71.42
4	12413	9754	2659	78.60
5	12413	10644	1769	85.75
6	12413	12413	0	100
7	12413	12413	0	100

위의 표에서 보듯이 임계값의 적용에 탐지율이 달라지는 것을 볼 수 있다. 장기간의 실험을 거쳐 최적의 임계치를 도출하였다. 본 논문에서는 이러한 탐지율을 바탕으로 TCP 트래픽 분석 알고리즘의 임계값은 5, UDP 트래픽 분석 알고리즘의 임계값은 3 그리고 ICMP 트래픽 분석 알고리즘의 임계값은 7로 적용하여 공격을 탐지 하였다. 이러한 임계값을 적용한 실험 결과 그림 6, 그림 7, 그림 8과 같다.

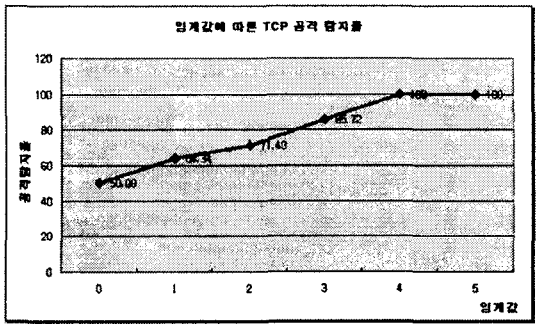


그림 6. 임계값에 따른 TCP 공격 탐지율

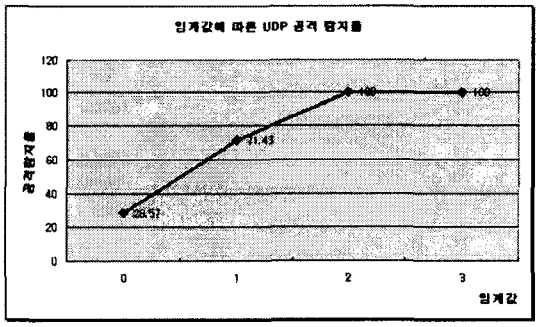


그림 7. 임계값에 따른 UDP 공격 탐지율

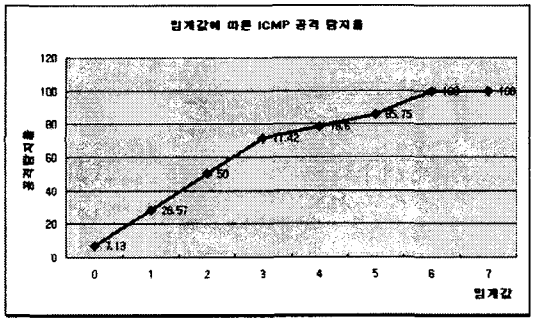


그림 8. 임계값에 따른 ICMP 공격 탐지율

위의 임계값을 수집된 각 포트별 트래픽에 적용하여 정상 트래픽과 공격 트래픽을 분석하게 되고, 이렇게 분석된 데이터를 실시간으로 보고 대응하기 위해 웹기반에서 그래프로 나타내었다. 최종적으로 관리자가 웹으로 확인하는 결과는 그림 9와 같다.

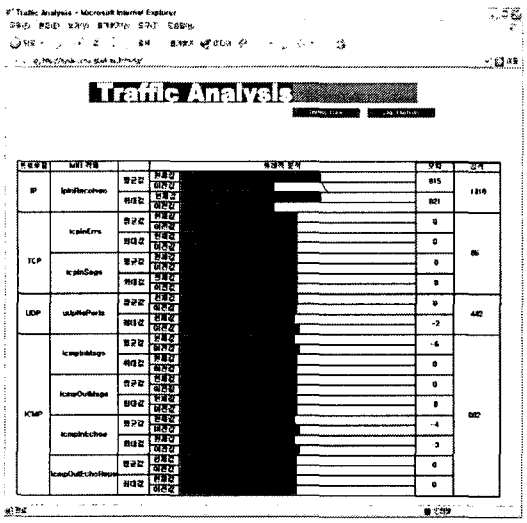


그림 9. 트래픽 분석 결과

IV. 결론

본 연구에서는 트래픽 폭주 공격에 대비하여 근본적으로 트래픽 폭주 공격의 차단과 네트워크 및 시스템의 자원을 보호하기 위한 목적으로 SNMP를 이용한 트래픽 폭주 공격 검출 알고리즘을 제안하고 구현하였다. SNMP의 여러 MIB 객체 중 실험을 통하여 선정된 MIB 객체를 중심으로 트래픽에 대한 분석 결과 각 트래픽 폭주 공격에 대한 특성을 도출하였고, 도출된 공격 트래픽 특성을 이용하여 분석 및 검출하는 알고리즘을 제안하였다. 제안된 SNMP를 이용한 트래픽 폭주 공격 검출 알고리즘은 실험의 결과로 확인하였다. 본 연구을 통하여 얻어진 알고리즘은 기존의 트래픽 검출 알고리즘 보다 정확한 트래픽 분석 및 대응을 할 수 있음을 실험을 통하여 확인하였다.

참 고 문 헌

[1] E. Lemonnier, "Protocol Anomaly Detection in Network based IDSs," Defcom, 2001.

[2] J. Case, M. Fedor, M. Schoffstall, J. Davin, "A Simple Network Management Protocol," RFC1157, 1990.

[3] J. Criscuolo "Distributed Denial of Service Trin00, Tribe Flood Network, Tribe Flood Network 2000 and Stacheldraht," CIAC-2319.

[4] F. Baker, K. Chan, A. Smith, "Management Information Base for the Differentiated Services Architecture," RFC3289, 2002.

[5] S. Waldbusser, "Remote Network Monitoring Management Information Base," RFC1757, 1995.

[6] K. McCloghire, F. Kastenholz, "The Interface group MIB," IETF RFC2863, 2000.

[7] K. McCloghrie, M. Rose, "Management Information Base for Network Management of TCP/IP-based internets," RFC1156, 1990.

[8] 최재원, "웹 기반 네트워크 트래픽 분석 시스템", 한국정보처리학회 학술발표논문집, 제7권, 제2호, 2000.

김 선 영(Sun-Young Kim) 준회원

2001년 3월 : 한밭대학교 전자공학과 (공학사)

2003년 2월 : 충북대학교 컴퓨터공학과 (공학석사)

2003년 3월 ~ : 충북대학교 컴퓨터공학과(박사과정)

<관심분야> : 인터넷 정보보호, 네트워크보안, 네트워크

박 원 주(Won-Ju Park) 정회원

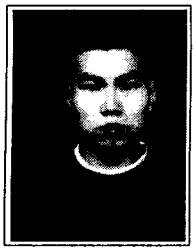
1998년 2월 : 충남대학교 정보통신공학과 (공학사)

2002년 2월 : 충남대학교 정보통신공학과 (공학석사)

2000년 2월 ~ : 한국전자통신연구원 연구원

<관심분야> : 인터넷 정보보호, 컴퓨터 통신, 네트워크

유 대 성(Dae-Sung Yoo) 준회원



2003년 2월 : 충북대학교 컴퓨터공학과 (공학사)
2003년 3월 ~ 현재 : 충북대학교 컴퓨터공학과(석사과정)

<관심분야> : 인터넷 정보보호, 네트워크보안, 네트워크

서 동 일(Dong-Il Seo) 정회원

1989년 2월 : 경북대학교 전자공학과 (공학사)
1994년 2월 : 포항공과대학교 정보통신공학과(공학석사)
2003년 3월 ~ 현재 : 충북대학교 전자계산학과(박사과정)
1994년 ~ 현재 : 한국전자통신연구원 선임연구원

<관심분야> : 인터넷 정보보호, 컴퓨터 통신, 네트워크

오 창 석(Chang-Suk Oh) 종신회원

1978년 2월 : 연세대학교 전자공학과 (공학사)
1980년 2월 : 연세대학교 전자공학과 (공학석사)
1988년 8월 : 연세대학교 전자공학과 (공학박사)
1985년 ~ 현재 : 충북대학교 전기전자컴퓨터공학부 교수
1982년 ~ 1984년 : 한국전자통신연구원 연구원
1990년 ~ 1991년 : 미국 Stanford대학교 객원교수

<관심분야> : 컴퓨터 네트워크, 뉴로 컴퓨터, 정보 보호