韓國 컴퓨터情報學會 論文誌
第10卷 第4號, 2005. 9.

2005-10-4-1-19

유해 트래픽 분석을 이용한 침입 방지

장 문 수*, 구 향 옥**, 오 창 석***

Intrusion Prevention Using Harmful Traffic Analysis

Moon-Soo Chang *, Hyang-Ohk Koo **, Chang-Suk Oh ***

요 약

컴퓨팅 기술과 네트워크 기술의 지속적인 발전은 인터넷의 폭발적인 성장을 가져왔으며, 사회 전반에 걸친 기반시설 및 공공 인프라, 산업 인프라 및 문화 환경을 인터넷 기반으로 변화시키는 중요한 역할을 수행했다. 최근 정보통신의 급속한 발전으로 인터넷을 이루는 컴퓨터 및 네트워크 환경은 초유의 성장과 발전을 거듭했지만, 잠재적인 취약점을 많이 가지고 있다. 이러한 취약점을 이용한 웜 및 해킹으로 인한 피해는 날로 심각하다. 본 논문에서는 이런 문제점들을 해결하기 위하여 유해 트래픽 분석 시스템을 설계하여 새로운 공격에 대한 방어와 네트워크의 트래픽을 분석함으로써 침입 및 유해 정보 여부를 판단하여 실시간으로 대응한다.

Abstract

The continuous development of computing technique and network technology bring the explosive growth of the Internet, it accomplished the role which is import changes the base facility in the social whole and public infra, industrial infrastructure, culture on society-wide to Internet based environment. Recently the rapid development of information and technology environment is quick repeated the growth and a development which is really unexampled in the history. but it has a be latent vulnerability. Therefore the damage from this vulnerability like worm, hacking increases continually. In this paper, in order to resolve this problem, implement the analysis system for harmful traffic for defending new types of attack and analyzing the traffic takes a real-time action against intrusion and harmful information packet.

▸ Keyword : Harmful Traffic, Traffic Analysis, Intrusion Prevention

---

• 제1저자 : 장문수
• 접수일 : 2005.07.27, 심사완료일 : 2005.08.22
* 충북대학교 전기전산공학과 , ** 충북대학교 컴퓨터공학과, *** 충북대학교 전기전자컴퓨터공학부

Ⅰ. 서 론

네트워크의 발달은 인터넷상에 접속된 컴퓨터가 데이터 뿐만 아니라 음성, 영상 등의 멀티미디어 정보를 취급하도록 하였다. VoIP, 인터넷 방송 등으로 컴퓨터, 통신, 방송의 융합이 현실화 되고 있으며, 초유의 성장을 거듭하여 사이버 공간이 아닌 차세대 네트워크 컨버전스(NGcN), 광대역 통합망(BcN)을 통한 디지털 네트워크로 현실화되고 있다. 그러나 인터넷을 이루는 컴퓨터 및 네트워크 환경은 잠재적인 취약점을 내포하고 있다. 이러한 취약점을 이용하여 웜, 바이러스, 해킹 등의 악의적인 목적으로 유해 트래픽 발생 및 공격으로 인한 업무장애, 불건전 정보 유통의 증가, 사생활 침해 등 정보화의 역기능이 폭발적으로 증가하여 크나큰 문제가 아닐 수 없다.[1]

이에 본 논문에서는 이러한 네트워크 환경 변화와 문제점을 해결하기 위한 방법으로 네트워크의 트래픽을 분석하여, 침입 혹은 유해 정보 여부를 판단하여 웜이나 DDoS와 같은 유해 트래픽 흐름을 탐지하고 차단할 수 있는 기능을 구현하여 적용하였다. 이를 통해서 기존 방법의 문제점을 찾아 개선할 수 있었으며 공격 트래픽과 같은 유해 트래픽에 대한 탐지율과 방지율을 향상시켜 신뢰성 있는 트래픽 흐름을 유도하여 안정된 네트워크 환경을 구성할 수 있었다.

본 논문의 구성은 기존 시스템의 트래픽 탐지 방법에 대하여 알아보고, 제안 시스템의 탐지율과 방지율을 기존 시스템과 비교하였으며, 실험한 결과를 토대로 결과를 고찰하였다.

Ⅱ. 기존 시스템의 트래픽 탐지 방법

기존의 트래픽 탐지 방법은 네트워크로 유입되는 트래픽을 수집하여 외부의 침입 위험으로부터 내부 네트워크를 보호하고 방화벽을 우회하는 공격이나 내·외부 네트워크로부터 위험을 사전에 탐지하는 시스템이다. 이때 트래픽 필터가 제대로 이뤄지지 않아서 발생하는 유해 트래픽 유입 문제와 오탐지에 의한 잦은 경보작동으로 인하여 관리자로 하여금 엄청난 불편을 초래하였다.[2] (그림 1)은 기존 시스템의 트래픽 탐지 모니터링 구성 요소를 나타내며 호스트 및 네트워크로부터 트래픽을 수집한 후 트래픽 가공 및 축약 단계를 거쳐 유해 트래픽에 대하여 침입 분석 및 탐지를 수행하며 보고 및 관리자에게 알리는 형태의 대응을 수행한다.

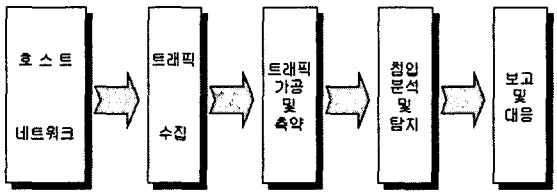


그림 1. 기존의 시스템 트래픽 모니터링
Fig. 1. Conventional Traffic monitoring

기존의 시스템에서의 트래픽 모니터링은 침입 탐지 모델을 기반으로 하기 때문에 오용 탐지와 비정상 행위 탐지의 경우 false negative 오류를 줄일 수 있었다. 하지만, 정상 행위 프로파일에 침입 및 유해 트래픽이 포함될 수 있으며 주기적인 행동 프로파일의 갱신이 필요하게 되므로 갱신이 지연되었을 경우 및 실시간으로 발생되는 유해 트래픽 패킷을 대상으로 시간대비 탐지율이 현저하게 낮아져 안정성이 떨어지는 것을 확인 할 수 있었다.

표 1. 탐지 모델에 따른 침입 탐지 시스템의 분류
Table 1. Classification of the intrusion detection system according to the detection model

구분	침입탐지방법
오용 탐지	조건부 확률
	전문가 시스템
	상태 전이 분석
	키 입력 감시
	모델 기반 침입탐지
비정상 행위 탐지	통계적 접근
	특징 추출
	비정상 행위 측정 방법의 절차
	예측 가능한 패턴 생성
	신경망

침입 탐지 모델에 따른 침입 탐지 방법은 〈표 1〉과 같다. 오용 탐지 모델은 이미 알려져 있는 공격에 대한 취약점 정보와 감사 데이터를 비교하여 침입을 탐지하는 시스템이고 비정상 행위 탐지 모델은 사용자의 비정상 행위나 컴퓨터 자원의 사용을 탐지하는 것으로 정상적인 행동 프로파일 모델을 벗어나는 경우를 침입으로 간주한다.

오용 탐지 모델은 취약점 규칙 정보를 갱신함으로써 알려진 취약점에 대하여 false positive 오류를 줄일 수 있고 비교적 구현 방법이 수월하다는 장점이 있어 대부분의 상용 침입 탐지 시스템에서 이용하는 기법이지만, 취약점 정보에 대한 의존도가 매우 높아 새로운 유해 트래픽에 대해서는 탐지하지 못하는 단점이 있다.

비정상 행위 탐지 모델은 알려지지 않은 새로운 형태의 유해 트래픽에 대해서도 대응 가능한 기법으로 오용 탐지 모델에 비해 false negative 오류를 줄일 수 있는 장점이 있지만 정상적인 트래픽에 유해 트래픽이 포함되므로 상당한 주기의 프로파일 갱신이 필요한 단점이 있다.

III. 유해 트래픽 분석을 이용한 침입 방지

본 논문에서 제안한 유해 트래픽 분석 시스템은 (그림 2)와 같다. (그림 2)는 단계별 유해 트래픽 분석 과정을 나타낸다. 1단계로 라우터의 패킷 필터링을 통하여 수집된 패킷을 대상으로 하며 2단계로 네트워크 취약점 분석을 분석하여 생성된 트래픽을 이용하여 BPF(Berkeley Packet Filter) 연산식을 적용, 규칙을 기반으로 한 트래픽 모니터링을 한다.[3] 2단계를 통해 필터링 된 네트워크 트래픽을 대상으로 2단계에서 생성되고 지속적으로 갱신되는 네트워크 취약점 분석 데이터베이스와 비교 검색하여, 취약성 여부를 판단하며, 유입되는 네트워크 트래픽을 대상으로 모니터링을 한다. 3단계에서는 유해 트래픽 및 정상적인 트래픽을 분석한다. 정상적인 트래픽의 경우에는 내부 네트워크로 안전하게 전달되지만, 유해 트래픽의 경우에는 유해 트래픽 차단 프로세스에 의해 내부 네트워크로 유입되기 전에 차단된다.

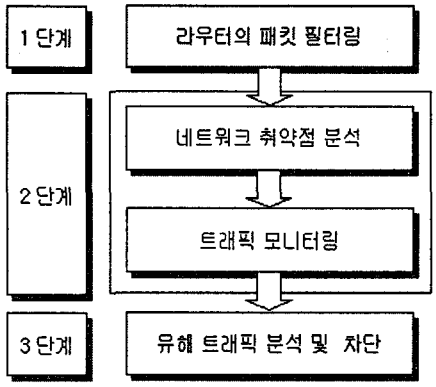


그림 2. 유해 트래픽 분석 절차
Fig. 2. Procedure of the harmful traffic analysis

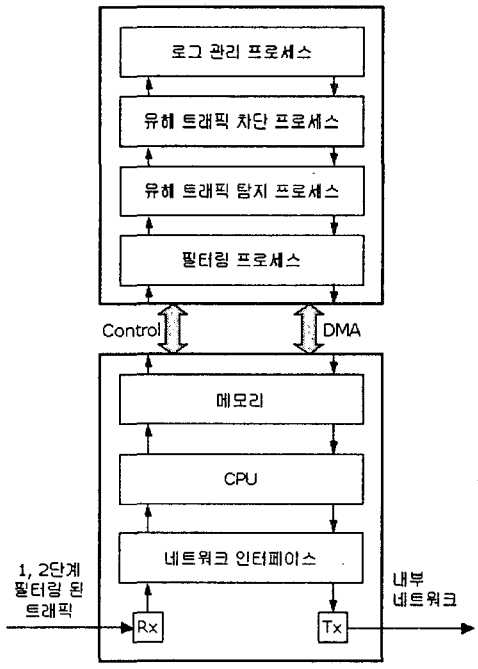


그림 3. 제안한 시스템의 기능도
Fig. 3. Functional structure of the proposed system

제안 시스템 구성은 네트워크 인터페이스를 통해서 유입되는 패킷을 필터링하는 프로세스와 유해 트래픽을 탐지하는 프로세스, 유해 트래픽을 차단하는 프로세스, 로그 관리 프로세스로 구성되어 있다. 이들 프로세스는 각각의 독립 프로세스로서 Thread 형태로 구성되어 있으므로, 실시간으로 수집된 패킷을 바탕으로 유해 트래픽 탐지 및 차단을 수행한다.

필터링 프로세스 단계에서는 BPF(Berkeley Packet Filter) 연산식을 적용하여 엄청난 양의 트래픽을 대상으로 트래픽 필터링을 진행하며, 유해 트래픽 탐지 프로세스는 필터링 된 트래픽을 기반으로 취약성 데이터베이스를 통해서 취약성을 판단하고, 유입되는 트래픽의 취약성에 따라 지속적으로 갱신하여 취약성 데이터베이스를 항상 최신의 정보로 유지하여 신뢰성을 확보한다.[4] 유해 트래픽 차단 프로세스는 유해성 판단 여부에 따라 해당 패킷을 차단하거나 내부 네트워크로 전송한다. 각각의 진행 사항은 로그 관리 프로세스에 의해 로그 데이터베이스에 축적되며, 향후 보고서 작성으로도 활용된다. (그림 3)은 제안 시스템 구성을 나타낸다.

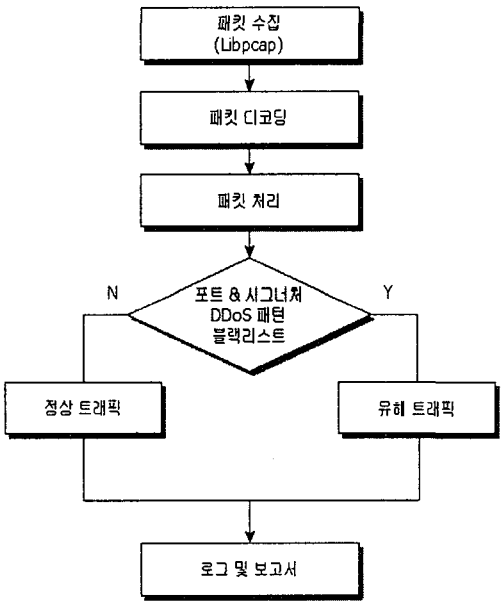


그림 4. 트래픽 분석 절차
Fig. 4. Procedure of the traffic analysis

트래픽 차단 절차는 Ethernet 인터페이스에서 모든 트래픽을 볼 수 있도록 하는 "promiscuous mode" 기능을 설정하여 라우터로부터 내부 네트워크로 유입되는 모든 트래픽을 대상으로 트래픽 분석을 실시한다[4]. 이때 엄청난 양의 트래픽 때문에 시스템에 과부하가 발생하게 되므로 BPF 연산식을 적용하여 필터링을 수행한다. 수집된 트래픽은 필터링이 완료된 후 2단계에서 취약점 점검으로 생성된 웜 관련 port 테이블, 시그너처 테이블, DDoS 패턴 테이블, 블랙리스트 테이블과 비교 검색된다. (그림 4)는 트래픽 분석 절차를 나타낸다.

(그림 4)에서의 트래픽 분석 절차와 같이 정상 트래픽일 경우에는 로그 관리 프로세스를 통해 로그 데이터베이스에 로그 정보를 저장한 후 내부 네트워크로 전송되며, 유해 트래픽으로 판단될 경우에는 로그 데이터베이스에 로그 정보를 저장한 후 차단되어 내부 네트워크로의 진입을 원천적으로 봉쇄하여 신뢰성 있는 네트워크 트래픽을 유지하고, 관리한다.

Libpcap, Libnet을 사용하여 네트워크 트래픽 정보를 수집하고 Nmap, Nessus를 통하여 네트워크 취약점 점검을 통하여 취약점 데이터베이스를 실시간으로 관리하고, 네트워크로 유입되는 패킷을 대상으로 유해 트래픽 여부를 판단하여 유해트래픽은 탐지 및 차단하며 정상적인 트래픽의 경우에는 내부 네트워크로 전송한다. (그림 5)는 트래픽 분석 절차를 나타낸다.

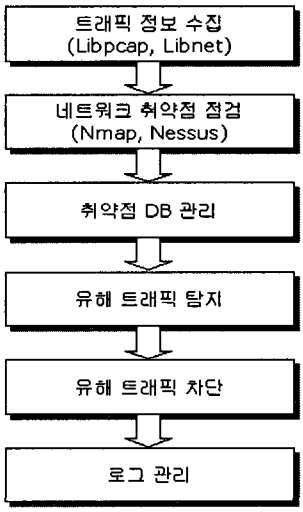


그림 5. 트래픽 차단 절차
Fig. 5. Traffic prevention process

트래픽 테이블 관리는 Libpcap을 통하여 수집된 네트워크 패킷을 MySql과 연동하여 저장된다. 일반 트래픽 테이블의 구성은 TCP/IP 프로토콜에서 IP 헤더 구조 중 프로토콜, 출발지 주소, 목적지 주소를 참조하며, TCP/UDP 헤더 구조에서 출발지 포트, 목적지 포트 번호를 참조하였다.[6] 또한 수집된 패킷의 전체길이와 패킷의 프로토콜을 나타내는 타입정보와 트래픽이 수집된 시간 정보로 구성되어 있다. 〈표 2〉는 일반 트래픽 테이블의 스키마 구조를 나타낸다.

표 2. 일반 트래픽 테이블의 스키마
Table 2. Schema of general traffic table

필드이름	필드형식	내용
psize	smalint(5)	패킷의 전체 길이
ptype	tinyint(3)	패킷이 프로토콜
sip	varchar(15)	출발지 주소
dip	varchar(15)	목적지 주소
sport	smalint(5)	출발지 포트 번호
dport	smalint(5)	목적지 포트 번호
logtime	datetime	패킷 수집 시간

트래픽 테이블에 수집된 트래픽 데이터는 웜 관련 port 테이블, 시그너처 테이블, DDoS 패턴 테이블, 블랙리스트 테이블과 비교 대상이 되며, (그림 3)에서 필터링 프로세스, 유해 트래픽 탐지 프로세스, 유해 트래픽 차단 프로세스에서 활용된다.

Ⅳ. 실험 및 결과 고찰

본 논문에서 제안한 알고리즘을 적용한 유해 트래픽 분석 시스템의 성능을 평가하기 위하여 약 2일 정도의 기간동안 수집된 네트워크 트래픽과 공격 프로그램으로 생성된 패킷을 기반으로 실험하였다.

취약점 점검 및 유해 트래픽 분석 시스템은 Libpcap과 Libnet을 통해서 실시간으로 트래픽을 수집하며, Snort, Nmap, Nessus를 통해서 취약점을 분석한 후 유해 트래픽 차단 프로세스를 통해서 차단한다. 트래픽 분석 모니터링은 SNMP 에이전트를 기반으로 하여, MRG를 이용 트래픽 흐름을 웹 브라우저를 통해서 결과를 확인하였다. 공격 시스템의 공격 도구로는 NetBus, Trin00, TFN, 패킷 발생기를 사용하였다.

(그림 6)은 실험 환경 구성을 나타낸다. 실험 환경 구성은 공격 시스템 영역, 라우터 영역, 공격 트래픽 모니터링 영역, 유해 트래픽 분석 시스템 영역, 유해 트래픽 차단 후 트래픽 모니터링 영역으로 나눈다. 2개의 더미 허브를 사용하여 허브로 유입되는 모든 트래픽을 대상으로 트래픽을 수집하여 각 단계별로 트래픽을 모니터링 한다.

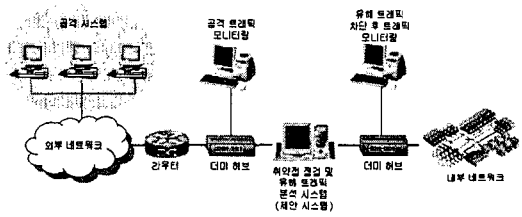
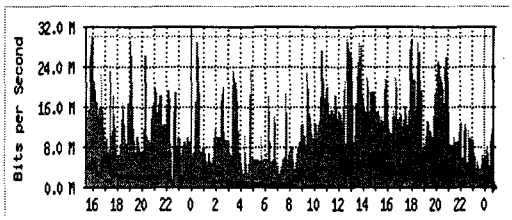


그림 6. 실험 환경 구성
Fig. 6. Configuration of the experimental environment

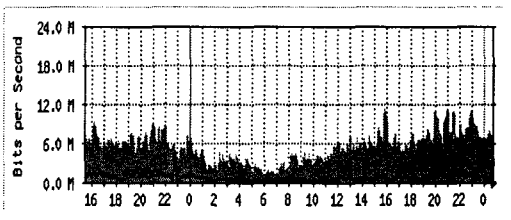
공격 시스템 영역에서는 공격 트래픽을 발생하여 목표로 하는 내부 네트워크로 공격 트래픽을 보내는 과정을 수행한다. 라우터 영역에서는 라우터 필터링 정책에 따라 라우터로 유입되는 패킷이 필터링되어 제안 시스템으로 유입된다.

(a)는 유해 트래픽을 발생하여 일반 트래픽과 함께 기존 시스템을 통과한 후의 트래픽을 모니터링 한 상황을 나타낸다.



(a) 기존 시스템

(b)는 제안 시스템인 유해 트래픽 분석 시스템을 통과한 후의 트래픽을 모니터링 한 상황을 나타낸다.



(b) 제안 시스템의 트래픽 모니터링

그림 7. 트래픽 모니터링 결과
Fig. 7. Result of the traffic monitoring

(b)에서 보는 봐와 같이 유해 트래픽이 현저하게 낮아졌음을 알 수 있다. 또한 안정적인 트래픽 흐름으로 원활하게 서비스되고 있다는 것도 파악할 수 있다.

실험 결과를 통하여 기존 시스템과 제안 시스템의 유해 트래픽 탐지율을 비교해 보면 (그림 8)와 같다. 제안 시스템을 적용한 경우에는 83.06%의 탐지율이 발생했으며, 기존 시스템에서 발생된 탐지율은 75.53%이다. 이것은 제안 시스템이 기존 시스템보다 탐지율 면에서 7.53% 향상된 성능을 가져왔다고 알 수 있다.

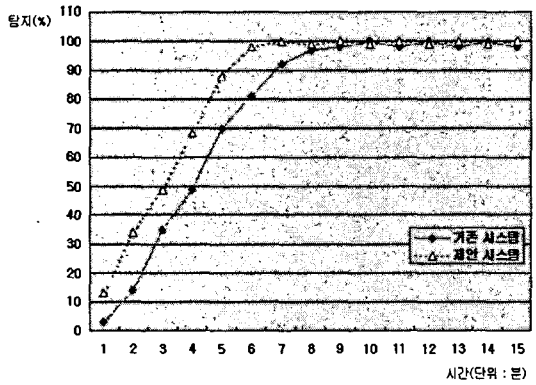


그림 8. 공격 탐지율
Fig. 8. Attack detection ratio

(그림 8)는 기존 시스템과 제안 시스템과의 탐지율 비교를 나타낸다.

기존 시스템과 제안 시스템의 유해 트래픽을 차단하는 방지율을 비교해 보면 (그림 9)과 같다. 기존 시스템에서 발생한 방지율은 17.13% 이다, 제안 시스템을 적용한 경우에는 52.26%의 유해 트래픽 방지 성능을 나타냈다. 이것은 기존 시스템에서 발생된 방지율보다 35.13%의 성능 향상을 가져왔다는 것을 알 수 있다.

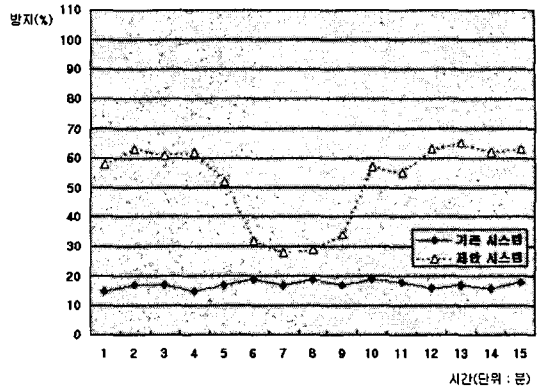


그림 9. 공격 방지율
Fig. 9. Attack prevention ratio

(그림 9)는 기존 시스템과 제안 시스템과의 방지율 비교를 나타낸다.

기존 시스템은 주로 침입 탐지에 의존하기 때문에 방지율에 대한 부분의 성능 비율이 상대적으로 낮다. 하지만 제안 시스템의 경우에는 탐지와 방지를 수행하기 때문에 방지율의 비율이 높다. (그림 9)의 제안 시스템을 보면 유해 트래픽 방지가 낮게 형성된 것을 알 수 있다. 이것은 내부 네트워크로 유입되는 트래픽에서 공격 트래픽만이 아닌, 정상적인 트래픽 구간을 나타낸다고 할 수 있다.

V. 결 론

본 논문에서는 네트워크로 유입되는 트래픽을 대상으로 유해성 여부를 판단하는 유해 트래픽 분석 시스템을 제안하여 웜이나 DDoS와 같은 유해 트래픽 및 비정상 트래픽의 흐름을 탐지하고 차단하는 기능을 구현하였다. 실험 결과를 통해 유해 트래픽에 대한 탐지율이 높아졌다는 것을 확인하였다. 무엇보다도 탐지된 유해 트래픽을 차단하는 정도가 기존 시스템에 비해 매우 높아졌다는 것을 확인할 수 있었으며, 이것으로 유해 트래픽으로부터 대응할 수 있는 네트워크 구성이 가능해졌으며, 보다 신뢰성 있고 안전한 네트워크 환경을 구성할 수 있었다. 향후 연구 과제로는 트래픽 조절과 시스템 성능에 따른 유해 트래픽 탐지와 방지의 효율성에 대한 연구가 이루어져야 할 것이다.

참고문헌

[1] 한국정보보호진흥원, 기업 정보보호 실천 가이드, 정보보호21c, 2004.

[2] 정보보호21c, 차세대 보안 솔루션 IPS 세미나, (주)인포더, 2004.

[3] 류승우, 해킹 보안 노트, 사이버 출판사, 2002.

[4] Jay Beale, Andrew R. Baker, Brain Caswell, Snort2.1 Intrusion Detection, Syngress Publishing, 2004.

[5] Michael Rash, Angela D. Orebauhg, Becky Pinkard, Intrusion Prevention And Active Response : Developing Network And Host IPS, Syngress Publishing, 2005.

[6] 오창석, 생동하는 TCP/IP 인터넷, 내하출판사, 2004.

저자소개

장 문 수

1997년 2월 충주대학교 전자계산학과(공학사)

2005년 8월 충북대학교 전기전산공학과(공학석사)

〈관심분야〉 정보보호, 컴퓨터 네트워크 차세대 네트워크 보안

구 향 옥

1999년 8월 한발대학교 전자계산학과(이학사)

2002년 2월 충북대학교 컴퓨터공학과(공학석사)

2002년~현재 충북대학교 컴퓨터공학과 박사과정

2003년 8월~현재 백석대학 겸임

〈관심분야〉 컴퓨터네트워크, 뉴로컴퓨터, 정보보호

오 창 석

1978년 2월 연세대학교 전자공학과(공학사)

1980년 2월 연세대학교 전자공학과(공학석사)

1988년 8월 연세대학교 전자공학과(공학박사)

1985년~현재 충북대학교 전기전자컴퓨터 공학부교수

1982년~1984년 한국전자 통신연구원 연구원

1990년~1991년 Stanford 대학교 객원교수

2001년~2004년 한국콘텐츠학회 논문지편집위원장

2004년~현재 한국콘텐츠학회 상임고문

〈관심분야〉 컴퓨터네트워크, 뉴로컴퓨터, 정보보호