네트워킹기능과 정보보호기능 연동기술 메커니즘 구현

노시춘* · 나상엽*

요 약

네트워크보안에서 네트워킹기능과 정보보호기능을 분리하여 관리하지 않고 연계하여 종합 메커니즘을 구성및 적용할 경우 종합적인 정보보호 효율은 시너지효과로 나타난다. 본 연구는 네트워킹 기능과 정보보호기능을 연계하여 정보보호기능을 적용했을 경우의 연동 메커니즘 구현 방법 개발과 그 성과를 측정하기 위한 것이다. 연동 메커니즘에의한 보안차단성과는 분리상황의 성과보다 8~10% 증대되어 나타난다. 따라서 네트워크 정보보호기능 구현은 반드시 네트워킹기능과 정보보호기능을 연계하여 구성하고 그 성과를 측정, 관리하는 것이 정보보호 성과 관리에 효율적 방법임을 본 연구를 통해 제시하고자 한다.

A Securing Method of Relational Mechanism Between Networking Technology and Security Technology

Sichoon Noh* · Sangyeob Na*

ABSTRACT

This paper related to implementing issue and performance measuring about blended mechanism between networking technology and security technology. We got more effectiveness in overall network security, when applying and composing amalgamated security mechanism between network technology and security technology. The blended method offers 8~10% effective result in network security than the isolated ways of applying relational two technologies. As a result, we suggest amalgamated security mechanism between network technology and security technology, and also, we propose the blended method as a model of more effective way.

Key words : Networking, Security, Mechanism

* 남서울대학교 컴퓨터학과 교수

1. 차단기능 연동구조 설계

1.1 네트워크 Layer별 공격패턴

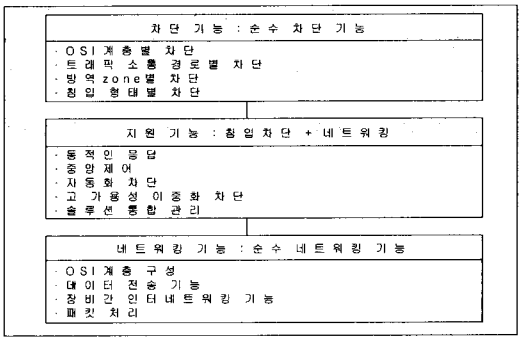
네트워크트래픽 처리과정에서의 기능 매커니즘 작동 과정을 설명하기 위해서는 OSI 계층별로 발생하는 보안 공격유형과 그 성격을 파악해야 한다. 최근의 해킹, 바이러스 공격은 OSI 계층 L2에서 L7까지 모든 계층에 걸쳐 발생하고 있다. 먼저 MAC 스푸핑(Spoofing)과 플러딩(Flooding)은 가장 대표적인 L2 레벨의 공격이다 이런 MAC 스푸핑과 플러딩이 백본 스위치까지 전달될 경우 네트워크 망 전체가 흔들리게 되며, 이를 이용한 공격이 늘어나고 있다. 다음으로 L3~L7 레벨의 공격으로 SYN 공격, 스푸핑, 플러딩이 대표적이다. 스머프(Smurf) 공격이 가장 대표적인 ICMP(Internet Control Message Protocol) 공격이고, 웰치아 웜은 애플리케이션 레벨의 ICMP 플러딩 공격이다. 2003년 1월 25일 발생한 SQL 웜은 UDP 플러딩의 대표적 공격 중 하나다. 사세르 웜은 DoS 공격의 한 형태로, 여기서 주목할 점은 DoS 공격을 의도하지 않은 사용자가 웜에 감염될 경우 자신의 의지와 상관없는 DoS 공격이 된다는 점이다.

1.2 연동구조 설계방향

네트워킹 기능과 정보보호기능은 기술영역 기준으로는 별도의 카테고리로 출발하지만 응용현장에서는 연동기능구조로 가동된다. 다양한 레이어별 네트워킹 공격에 대응하기 위해서는 양기능 연동구도에 의한 단계별 차단을 실시해야한다. 연동구조기능은 네트워킹기능, 효율성지원기능, 보안차단기능으로 구성되고 기능 수행과정은 스위칭 단계 → 침입차단시스템 필터링 단계 → 내부 게이트웨이 필터링 단계 → 서버 바이러스 월 차단단계 → 자동화 방역 단계 순서로 이루어진다.

1.3 종합메커니즘

종합 매커니즘 구조는 (그림 1)과같이 네트워킹 기능, 지원기능, 정보보호기능 3단계로 계층화된다. 네트워킹기능은 네트워크 인프라상의 통신트래픽처리 기능이다. 네트워킹 기능은 OSI 7 layer별로 차별화된 네트워킹 기능 구조를 형성하고 이 구조상에서 라우팅, 스위칭, 브로드캐스팅등 인터네트워킹 기능, 데이터 전송기능 그리고 패킷처리 기능을 수행한다. 다이어그램으로 본다면 이 네트워킹 기능 영역내에 지원기능과 침입차단 기능이 존재한다. 지원기능은 네트워킹 기능을 토대로 하지만 침입차단 기능 구현시 적용되어야 할 필수적인 효율성지원기능 또는 연관기능이다. 지원기능은 성격상 3개 세부 영역으로 분류되데 고가용성 기능, 통합관리 기능 및 자동화처리와 실시간처리 기능이다. 정보보호기능은 인프라구조상에서의 바이러스와 각종 악성코드 차단기능이다. 침입차단 기능은 OSI 계층별 차단, 트래픽 소통 경로별 차단, 방역 Zone별 차단으로 분류될 수 있다. OSI 계층별 차단은 OSI Layer2에서 Layer7까지의 계층별로 수행되는 차단 기능이다. 경로별 차단은 외부 라우터에서부터 최종 클라이언트까지의 트래픽 경로별로 수행되는 차단이다. 방역 Zone별 차단 기능은 각종 Resource별로 차단 기능이 수행되는 것이다.



(그림 1) 연동기능 종합메커니즘

1.4 스위칭과정 연동

1.4.1 컨텐츠 스위칭(Contents Switching) 연동

단위 네트워크 그룹에 유입되는 트래픽은 내부 외부 경계선에 위치한 외부 라우터(Exterior Router)를 통해 경로 배정과 포워딩이 이루어진 다음 최초로 스위칭 단계로 유입된다. 스위칭 단계에서는 네트워킹기능, 보안기능이 수행되고 더불어 효율성 기능이 구현된다. 스위칭기능은 L2에서 L7까지 수행된다. L2~L3까지의 기능은 일반적인 네트워킹 처리 과정의 트래픽 경로 배정과 부하 분산 기능을 위주로 수행한다. 즉 물리 주소, IP 주소, TCP 포트 번호를 기준으로 스위칭 기능이 수행된다. 해킹, 바이러스 차단 기능으로서의 본격적인 방역기능은 L4, L7 스위칭 기능을 통해 구현되는데 그 이유는 L4 이상의 상위 계층 스위칭은 IP 주소, TCP 포트 번호를 기준으로 가동되고 특히 L7 스위칭은 패킷의 특정 URL 정보, 제목, 내용을 나타내는 검색어 등 소위 컨텐츠를 기준으로 스위칭되기 때문이다. 따라서 L7 스위칭을 상위계층 스위칭이라고 분류하며 해킹, 바이러스 침투를 차단하는 기능으로서는 특히 L7 스위칭 기능을 채택한다.

1.4.2 유입 트래픽의 스위칭 연동

외부 라우터(Exterior Router) 이후 침입차단시스템 전단에 스위칭을 구성한다. 스위칭 목적은 전통적 기능인 부하 분산(Load Balancing) 기능 외에 컨텐츠 인식 기능을 갖는 Layer7 스위칭을 수행하기 위해서이다. 이 기능을 통해서 컨텐츠 기반 패킷필터링과 앤티바이러스 기능, 응용 레벨의 미러링(Mirroring)을 수행한다. 컨텐츠기반 패킷필터링 기능은 앤티바이러스 기능의 근간이 된다. 최근 기승을 부리는 님다, 코드레드, 마이둠 등 바이러스는 기존의 침입차단시스템 기능만으로는 해결하기 어렵고 스위치 단계에서 강력한 패킷 처리 능력과 인지 능력을 통해 보안 기능을 제공한다.

1.4.3 바이러스 필터링 연동

NBAR(Network-Based Application Recognition) 기능에 대해 설명하면 QoS(Quality of ervice)의 큐잉(Queuing) 방법 중에는 BWFQ(Class-based Weighted Fair Queuing)기능이 있다. CBWFQ는 특정 기준에 의해 트래픽을 류(Class-map)하고 분류한 트래픽에 대해 하나 혹은 그 이상의 정책을 적용(Policy-map) 하고 라우터의 인터페이스에 Policy-map을 적용한다. 따라서 Class-map을 어떻게 분류하는지 Policy-map을 어떻게 적용하는지, 인터페이스에 적용할 때는 어떻게 적용하는지 등 경우의 수가 많기 때문에 폭넓은 설정과 세심한 조정이 동시에 가능한 방법이다. NBAR는 CBWFQ를 이용해서 라우터에서 구현하기 어려운 여러 가지 기능을 제공한다. NBAR는 동적 TCP/UDP 포트를 사용해서 분류하기 힘든 프로토콜이나 웹 기반의 프로토콜 등과 같이 다양한 애플리케이션을 인식할 수 있는 분류 엔진(Classification Engine)이다. NBAR는 다음과 같이 몇 가지 분류 기능이 있다. 동적으로 할당된 TCP, UDP 포트 번호를 가진 애플리케이션 분류, URL, HOST, MIME(Multipurpose Internet Mail Extension)타입에 의한 HTTP 트래픽의 분류, 애플리케이션 이름에 의한 ICA Independent Computing Architecture)분류 등이다. 이 중에서 'URL, HOST, MIME 타입에 의한 HTTP 트래픽의 분류' 방법을 이용해 코드레드, 님다 등과 같은 웜 바이러스 형태의 공격을 라우터에서도 차단할 수 있다]. NBAR는 애플리케이션 트래픽을 TCP/UDP 포트 번호 이상으로 분석할 수 있다. 이것을 서브포트 분류(Sub-port Classification)라고 한다. NBAR는 TCP/UDP Payload 자체를 들여다보고 트랜잭션 식별자, 메시지 타입, 다른 유사한 데이터와 같은 내용물에 따라 패킷을 분류한다. URL, HOST 또는 MIME 타입 등은 HTTP 트래픽에서 Get 요청시 URL이나 HOST 필드내에 있는 규칙적으로 나오는 텍스트에 의해 HTTP 트래픽을 분류할 수 있다.

1.5 침입차단 필터링 연동

침입차단시스템 처리단계에서 바이러스를 체크하는 기능을 침입차단시스템 스캐닝이라 한다. 침입차단시스템은 패킷 단위를 어떤 타입의 트래픽이며 어디에서 발신되고 목적지가 어디인지를 기준으로 접근을 통제한다. 일반적으로 침입차단시스템을 필터링 라우터로 그 기능이 대표되고 있다. 광범위하게 바이러스를 진단하고 보다 정교한 수준의 필터링 기능을 수행하기 위해서는 패킷 타입을 조사하고 분석 작업을 수행할 수 있어야 한다. 이러한 기능은 일반적으로 프록시(Proxy)나 애플리케이션 서비스(Application Service)로 제공된다. 프록시 서버는 클라이언트와 원격의 애플리케이션 서버 사이에 삽입된다. 그러나 이러한 침입차단시스템은 필터링과 프록시 서비스 모두 유지 가능하다. 일반적으로 침입차단시스템은 서비스(www, 텔넷, FTP, Mail 등)를 제공하는 네트워크 환경에서 해당 서비스를 요청한 호스트의 주소와 포트번호 그리고 사용자 인증 등의 기능을 기반으로 통제하게 된다. 정상적인 사용자에게는 요청한 서비스를 제공하고 허용되지 않은 사용자에게는 서비스를 차단하여 내부 네트워크로의 접근을 통제하게 된다. 침입차단시스템의 주요 기능은 내부 외부 네트워크의 유일한 연결점으로서 기능을 수행하면서 서비스 허용 및 차단, 사용자 인증 그리고 내 · 외부 상호 접속된 네트워크에 대한 트래픽 모니터링을 수행하는 것이다.

1.5.1 프록시 서버(Proxy Server) 기능연동

프록시는 클라이언트와 실제 서버 사이에 존재하며 둘 사이의 프로토콜 및 데이터를 중계하는 역할을 한다. 프록시는 전송자 또는 전달자라고도 한다. 프록시 기능을 이용하는 침입차단시스템은 애플리케이션 침입차단시스템과 서킷 게이트웨이 침입차단시스템이 있다. 프록시 서버 동작 과정은 클라이언트가 침입차단시스템으로 접속을 요구하면 침입차단시스템상의 프록시 서버는 접속 허용 규칙을 이용하여 클라이언트의 접속 여부를 결정한다. 만약 접속이 거부되면 연결을 끊고 접속이 허용되면 프록시 서버가 실제 서버로 접속을 요구하여 프록시 서버와 실제 서버건의 연결을 맺는다. 또한 프록시는 클라이언트로 접속 요청에 대한 응답을 보내어 클라이언트와 프록시 서버간의 연결을 맺는다. 이렇게 연결이 설정된 프록시는 클라이언트와 서버 사이에서 전달자 역할을 수행하게 된다. 일단 접속이 이루어지면 사용자는 프록시 서버를 거치지 않고 직접 연결이 된 것으로 생각하게 된다. 프록시 침입차단시스템은 바이러스 스캐너(양쪽 프로그램의 타입은 기본적으로 필터)와 같은 기능을 수행한다. 그러나 침입차단시스템에 의해서 이루어지는 분석은 입력 스트림을 바이트 단위로 읽는 스캐너가 하는 것과 같지는 않다. 원칙적으로 침입차단시스템은 전체 스트림의 상세보다는 소스 어드레스, 수신국 주소, 포트 번호에 대해서 패킷을 검사한다. 바이러스 스캐닝을 추가하는 것은 전체적으로 네트워크 접속 시간이 상당히 느려지게 할지도 모른다.

1.5.2 애플리케이션 레이어 트래픽 분석과 차단기능 연동

프록시 서버에서는 패킷 필터링을 통과한 패킷에 대해 Store-and-forward 트래픽 뿐만 아니라 쌍방향 트래픽을 처리하게 되며 이때 애플리케이션 레이어에서 트래픽을 분석할 수 있도록 프로그램이 된다. 따라서 사용자 단계와 응용 프로토콜 단계에서 액세스 제어를 제공할 수 있고 응용 프로그램의 사용에 대한 기록을 통해 감사 추적(Audit)을 할 수 있게 된다. 응용 게이트웨이는 사용자 단계에서 들어오고 나가는 모든 트래픽에 대한 기록을 관리하고 제어할 수 있게 되며 인증을 받지 못한 사용자를 위해서는 별도의 인증 기법이 필요하게 된다. 응용 게이트웨이는 실제 서버의 관점에서 볼 때 클라이언트처럼 동작하며 클라이언트 관점

에서 볼 때는 실제 서버처럼 동작하게 된다. 응용 게이트웨이의 실현 예는 Telnet 게이트웨이, FTP 게이트웨이, Sendmail, NNTP(Network News Transfer Protocol) News Forwarder 등이 있다.

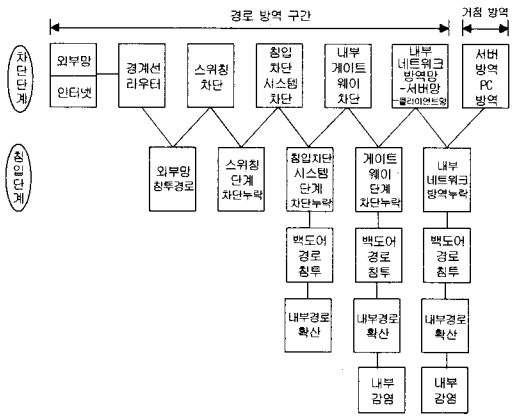
1.6 내부 게이트웨이 레벨기능 연동

바이러스 방역에는 오염 사이트로부터 유입되는 트래픽 필터링이 매우 중요하다. 바이러스 감염으로부터 데이터를 보호하기 위해서는 바이러스가 네트워크 상 핵심 중요 정보에 도달하기 전에 실시하는데 웹 트래픽과 SMTP 트래픽을 대상으로 한다. 통계에 의하면 일반적으로 전체 트래픽에서 차지하는 비중은 웹 트래픽이 80%, SMTP 트래픽이 10%로 나타난다. 따라서 이 두 개 종류의 트래픽에 대해 사전 방역을 실시하는 방안은 바이러스 차단과 Performance 향상 두 가지 측면에서 매우 긴요하다[3-3]. 게이트웨이 방역의 기본 기능은 필터링 기능이다. 게이트웨이에서 적용할 수 있는 필터링 종류는 바이러스 필터링, 컨텐츠 필터링, 이메일 필터링, 파일 필터링, 스팸 필터링 등으로 구분할 수 있다. 바이러스 필터링은 패킷 단위로 바이러스 감염 여부를 점검 삭제하며 컨텐츠 필터링은 이메일의 제목과 본문내용에서 특정 키워드가 발견되는 경우 이를 차단하는 기능이다. 이메일 필터링은 이메일 통과 허용 Size를 제한하는 기능이며, 파일 필터링은 특정 첨부 파일명이나 확장자를 미리 검사해 차단하는 기능이다.

1.7 보안차단 연동 메커니즘

모든 도메인 상에는 전 단계 도메인으로부터 발생되는 방역 누락 요소와 당해 도메인 상에서의 직접 감염 등 두 가지 유입 유형의 감염이 발생한다. 그리고 각 도메인 상에서 단 한건의 감염도 전체 도메인으로 확산된다. 따라서 각 도메인마다 차단 기능이 구현되고 차단 기능은 도메인간 연동되어야 한다. 차단 기능은 단계별로 연동된다. 연동이란 전 단계 도메인 차단 시 방역 누락되는 누수 바이러스를 다음 단계 도메인에서 차단하고 이 같은 방역 누락을 다음 단계 도메인에서 차단해주는 기능이 5단계 전 과정에서 구현되는 매커니즘을 말한다. 방역 누락은 방역 도메인별로 각기 다른 상황에서 발생된다. 첫 번째는 신종 바이러스와 악성 트래픽에의해 발생되는데 이 경우는 차단 장치상의 백신 엔진이 업데이트될 때까지 방역 누락이 계속된다. 그러나 백신 엔진이 업데이트된 이후에는 방역 누락이 발생치 않는다. 두 번째 단계인 침입차단시스템 필터링 단계에서도 또 다른 침투 유형이 등장하는데 바로 백도어 경로를 통한 악성 트래픽의 접속이다. 침입차단시스템을 우회하는 악성 트래픽이 침입차단시스템 하부 경로에서 발생된다. 또 하나의 침투는 내부 경로상에서 발생하는 악성코드, 바이러스의 존재이다. 이 역시 침입차단시스템 하부 경로에서 기동된다. 이 같은 세가지 패턴의 침입 유형은 그대로 내부 네트워크로 유입된다. 만일 내부 게이트웨이 필터링이 없다면 침투는 서버군과 클라이언트군으로 유입된다. 내부 게이트웨이는 내부 도메인 진입로 초기에서 악성코드 접속을 차단한다. 그다음의 침투 패턴은 또 다른 양상을 보이는 서버군에 대한 침투이다. 내부 게이트웨이 필터링에서 다시 방역 누락이 발생한 악성코드는 서버군과 클라이언트 군으로 진입한다. 또 다른 침투유형은 내부 매체 감염의 시작이다. 내부 네트워크중 서버와 클라이언트에서 감염을 일으킨 악성코드는 서버, 클라이언트군으로 진입하게 된다. 만일 서버 방역망이 없다면 이 같은 네 가지 패턴의 침투는 그대로 서버와 클라이언트 자원에 침투한다. 이상과 같은 5단계의 차단 기능 연동은 전 단계에서 발생된 새로운 형태의 침입을 다음 단계에서 차단하므로서 종합적인 차단 능 연동을 구현한다. 5개의 도메인을 대상으로 반드시 5단계 차단이 필요하고 만일 1단계 또는 3단계 차단 구조는 그만큼 미차단 도메인이 발생함으로서 위험성은 정비례하여 증가한다.

경로 방역 구조에서 5단계 차단이후에는 기존 방역 체계인 서버, 클라이언트 개별 방역이 시행될 수 있으나 본 논문에서의 연구범위가 아니므로 이에 대한 효과 분석을 생략한다. 다음그림은 차단 기능을 도메인간 연동 과정 측면에서 보여주고 있다.



(그림 2) 보안차단 연동 메커니즘

2. 연동기능 성과측정

2.1 연동기능 측정시스템 구성

선정한 시스템상의 측정용 에이전트 PC에서 출발한 트랜잭션은 Outbound 트래픽으로 사내 시스템인 클라이언트 → 서버 → 내부 게이트웨이 → 침입차단시스템 → 스위치 → 외부 라우터를 통과하여 인터넷 구간으로 접속된다. 이때는 네트워킹 기능단계이며 보안 메커니즘은 기동되지 않는다. inbound 트래픽은 인터넷 구간의 서버를 거쳐 인트라넷 구간인 외부 라우터 → 스위치 → 침입차단시스템 → 내부 게이트웨이가지 접속되고 내부 게이트웨이에서 서버 또는 클라이언트가지 접속된다. 이때는 보안처리 과정을 거치게 된다. 측정 시스템은 운용 시스템 상에서 발생되는 데이터를 빠짐없이 채집하고 이를 정확하게 분석할 수 있도록 하드웨어, 소프트웨어, 네트워크가 구성되어야하고 측정에 필요한 방법론인 검증용 화면 구성, 검증 조건 등이 설정되어야 한다

2.2 연동기능 차단효율성 분석

연동기능분석은 정보보호 방역성과 분석으로서 구체적으로 웜 바이러스 출현 시 S기업의 인트라넷 시스템상의 방역처리 실적으로 보여주고 있다. 다음의 <표 1>은 연동기능 적용후 6개월간 조사된 S기업의 전체적인 차단 성과를 하나의 표로 집계한 것이다. 이 기간중 발생한 웜 바이러스와 악성코드종류는 Blaster, Welchia, Agobot, Mydoom.A, Mydoom.B으로 채집되고 있으며 웜 바이러스 차단유형은 감염된 URL의 접속차단, 웜유입차단, 악성코드감염 트래픽과 Site 추적, 악성코드 감염 IP 추출 및 차단, 그리고 DDoS 방지로 나타났다. 악성코드 발생량과 차단실적은 조사가능 방법으로 집계된 것이며 조사된 사항은 발생실적대비 98% 차단실적을 나타내고 있다.

〈표 1〉 연동기능에의한 웜 종류별 차단실적

구분	Blaster	Welchia	Agobot	Mydoom.A	Mydoom.B
방역조치	· URL 차단 · Windows 업데이트 · COM차단 · DDoS 방지 · 웜 차단	· URL 차단 · www.microsoft.com 차단 · 감염 IP 추출 및 차단 · DDoS 방지 · 웜 차단	· URL 차단 · Dunghole.mysqld.com 접속시도 IP 추출 · DDoS 방지 · 웜 차단	· URL 차단 · www.sco.com 차단 · 감염 IP 차단 · DDoS 방지 · 웜 차단	· URL 차단 · www.microsoft.com 차단 · DDoS 방지 · 웜 차단
발생량	740,000건	143,000건	10,000건	480,000건	290,000건
차단실적	· 738,000건 차단 · 감염 트래픽과 Site추적	· 142,900건 차단 · 감염 IP 4,063개 추출	· 98,600건 차단 · 감염 IP 추이 분석	· 478,000건 차단 · 감염 IP 추출	· 289,000건 차단 · 감염 IP 추출

2.3 연동기능 차단유형별 방역효율

연동기능 효율분석은 네트워킹기능, 효율성지원

기능, 보안차단기능 수행구조상에서 연동기능 1단계 차단, 3단계 차단, 5단계 차단 유형별로 차단효과와 Latency를 각각 분석하고 그 결과를 종합 효율로서 평가하는 방법이다. 이상적 연동기능 차단구조 모델은 보안차단율은 높을수록 유리하고 Latency는 낮을수록 유리하다. 연동기능 1단계 차단의 경우는 1개 도메인의 방역만 가능하고 나머지 4개 도메인의 방역은 불가하다. 연동기능 차단단계가 다단계일수록 방역율은 높고 Latency는 증가한다. 종합 효율측면은 연동기능 다단계 차단 구조 적용시 전체적인 Performance에 지장을 초래하지 않고 차단기능이 수행된다. 즉 Performance 지연은 1단계 차단, 3단계 차단에서 미미한 정도이며 5단계 차단에서도 두드러지게 나타나지 않았다.

참 고 문 헌

[1] 김귀남, 노시춘, "다단계 바이러스 차단 구조 설계", 2004 한국 사이버테러 정보전 컨퍼런스, 2004.

[2] P. Denning, "Computer Under Attack Intruders, Worms and Virus", ddison Wesley, 1990.

[3] F. Cohen, "A short Course on Computer Viruses", ASP Press, 1990.

[4] 최의인, "악성코드의 분류 및 탐지 기법", 한남대학교, 2003.

[5] Lan Browde and Camille Smith, "Virus Protection", In De Sense, Inc, 1999.

[6] Rainer Link, "Server-Based Virus rotection on Unix/Linux", University of Applied Science Furtwamgan, Germany, 2003.

[7] Willam Stallings, "Network and Internetwork Security", Prentice Hall, 1995.

[8] J. Hruska, "Computer Virus and Anti-virus arfare", Ellis Horwood, 1992.

[9] David Mitchell and Katherine Carr, "Best Practice for multi-tier virus proctection", Oxford University, 2002.

노 시 춘

1987년 고려대학교 경영정보학(석사)
2004년 경기대학교 정보보호기술(박사)
1996년 KT IT본부 시스템보안부장
2004년 KT 충청전산국장
2005년~현재 남서울대학교 컴퓨터학과 컴퓨터 전공 교수
관심분야 : 차세대통신망, 정보보호, 컴퓨터네트워크

나 상 엽

1995년 동국대학교 컴퓨터공학과(공학석사)
2001년 동국대학교 컴퓨터공학과(공학박사)
2005년 Carnegie Mellon University School of Computer Science MSIT (Master of Information Technology)
1996년~현재 남서울대학교 컴퓨터학과 교수
관심분야 : 정보보호, 정보검색, 데이터 마이닝