MIB 기반의 보안 관리 시스템 모델에 관한 연구

구 자 환* · 박 병 연** · 유 기 성** · 이 행 곤** · 엄 영 익*

요 약

정보화 사회로의 이전에 따라 사회전반의 기반구조 및 경제 사회 활동이 정보통신 인프라에 의존하게 되고 기반구조와 운영 소프트웨어들의 취약점으로 인한 인터넷의 보안 문제는 많은 심각한 문제점들을 드러내고 있다. 특히 해킹 기법과 바이러스들이 점차 자동화, 지능화, 대중화, 분산화, 대규모화, 은닉화 되어감에 따라 이들에 대한 효과적이 대처 방안이 요구되어지고 있는 실정이다. 이에 본 논문에서는 점차 지능화 되어가는 네트워크 상의 위협들에 관해 조사 분석하고 이를 바탕으로 MIB 기반의 보안관리 시스템 모델을 제안하고자 한다.

A Study on the Model of MIB-based Security Management System

Ja-Hwan Koo* · Byung-Yeon Park** · Ki-Seong Yoo**
Haeng-Gon Lee** · Young-Ik Eom*

ABSTRACT

With the rapid adaption of the network technologies, there has been in continual troubles with network attacking and computer virus which are getting more automatic and intelligent. To solve them, we survey the existing and currently used security solutions, describe the architecture of traditional network management, and propose the model of a MIB-based security management system which has dedicated management information base on each security solution.

* 성균관대학교 정보통신공학부
** 한국과학기술정보연구원

1. 서 론

초고속통신망의 보급으로 우리나라는 선진국들과 비교하여 어느 나라보다도 정보통신 인프라 구축이 잘 되어 좋은 환경과 폭 넓은 사용자를 확보하고 있다. 2001년 말 현재 전자상거래 규모가 118조 원에 이르고 있으며, 인터넷 뱅킹의 계좌 수는 무려 1,131만 명, 인터넷을 통한 주식거래의 비중은 전체의 67%에 이르고 있는 실정이다.

그러나, 갈수록 늘어가고 있는 인터넷의 해킹 등 다양한 역기능에서 발생되는 문제점들을 해결하기 위해 정부에서는 국가 안보 차원의 사이버테러 대응 업무 수행을 위한 조직적인 대책 마련과 관련법과 제도 개선, 정보보안 역량 강화를 위한 인력 및 교육 방안과 보안 기술 및 정보보호 산업체들에 대한 산업 대책 등 다양한 중점 사항들에 대한 대책 마련에 고심하고 있다

정부뿐만 아니라 학계 산업계에서도 다양한 보안 솔루션을 제안하여 정보보안에 대한 해법을 제시하고 있지만, 지능화 되어가는 네트워크 침해를 막기에는 역부족인 실정이다. 본 논문에서는 매니저가 네트워크를 직접관리, 모니터링함으로써 보안의 질을 높이는 MIB-기반의 보안관리 시스템을 이용한 네트워크 보안 방안을 제시하고자 한다.

먼저 2장에서는 해킹 등 사이버 테러에 대한 간략한 소개를 하고 3장에서는 현재의 보안 솔루션의 형태를 정리한다. 마지막으로 4장에서는 MIB-기반의 보안관리 시스템의 구조와 동작에 대한 설명을 한다[1, 2, 5].

2. 사이버 상의 위협

정보화가 발전될수록 해킹, 바이러스 등 사이버 상의 위협은 점차 자동화, 지능화, 대중화, 분산화, 대규모화, 은닉화 되어 가는 경향을 띠고 있으며 단순한 실력 과시용 위협에서 점차적으로 악성화, 범죄화되고 있다. 이와 같이 해킹의 목적이 바뀌어 감에 따라 이에 대응하기 위한 새로운 방어 수단들이 개발되고 있으나 이를 무력화하거나 회피할 수 있는 해킹 기법들도 새롭게 나타나고 있다. 아래에서는 해킹 기법의 변천사와 변화되고 있는 해킹 동향들에 대해서 살펴본다.

2.1 해킹기술과 바이러스 기술의 통합화

기존에는 서버에 침입하거나 악성 코드를 관리자 모르게 설치하여 자료를 삭제하거나 시스템을 훼손시키는 등의 기법들을 많이 사용하였다. 그러나 최근의 피해 현황에서 볼 수 있듯이 코드레드(Cordred), 님다(Nimda), 클레즈(Klez), 프레템(W32.Frethem.J@mm) 등 웜 바이러스에 의한 피해가 많이 나타나고 있다.

2.2 시스템 공격에서 네트워크 서비스 공격으로 변모

앞의 해킹 기법 변화에서 알 수 있듯이 해당 특정 시스템을 침입하여 자료를 파괴하거나 획득하는 등의 시스템 공격에서 이제는 DoS나 DDoS, DRDoS 공격과 같이 트래픽을 대량으로 발생시켜 해당 서버나 라우터 등 네트워크 장비의 동작을 방해하거나 네트워크를 마비시킬 수 있어 특정 호스트를 목표로 하기보다는 네트워크 인프라스트럭처 자체에 대한 공격이 시도되고 있다.

2.3 Hacktivism 확산

해킹의 또 다른 변화는 개인적 단순한 목적에서 정치, 사회, 군사, 산업적 목적으로 변화되어 가고 있는 점이다. 핵티비즘이란 '해커(hacker)'와 행동주의를 뜻하는 '액티비즘(activism)'의 합

성어로 급진적인 정치·사회적 목적을 달성하기 위한 컴퓨터 해킹을 말한다. 온라인 상에서는 10명의 인원만 있어도 해당 사이트를 마비시키거나 해를 가할 수 있을 정도로 위력을 발휘할 수 있기 때문에 점차 소정의 목적을 위한 도구로 이용되는 사례가 늘고 있다.

2.4 웜 공격

최근 웜과 해킹 기법이 결합된 형태가 나타나고 있다. 근래의 피해 사례를 보면 순위에 올라있는 대부분의 수법들이 웜 바이러스에 의한 피해가 주를 이루고 있다. 최근의 프레덤.E(Frethem.E), 시멀리.D(Simile.D) 뿐만 아니라 코드레드, 님다, 클레즈 등의 웜 바이러스들이 불특정 다수의 컴퓨터와 사용자들에게 피해를 입히고 있다. 님다와 코드레드 웜의 경우 웜 바이러스와 전통적인 해킹 방식이 결합되어 나타난 형태로 복제와 확산을 위해 다양한 방식과 기법이 사용됐다. 또 이로 인해 알려진 취약점이 공개됐다. 님다의 경우 여러 가지 감염 방식이 사용되었으며, 다수의 전자우편 전송자처럼 움직이면서 취약한 웹사이트에서 복제를 수행했다. 그리고 감염된 웹사이트를 방문한 사용자들의 시스템에도 다운로드를 수행하였다. 감염된 해당 네트워크와 서버는 그 영향으로 마비되는 경우가 발생하여 업무에 막대한 지장을 초래하였다.

2.5 무선 해킹의 등장

최근 휴대폰 문자 메시지를 이용한 광고 발송으로 인한 프라이버시 침해가 늘어나고 있는 등 휴대폰과 PDA 등 무선 기기들의 등장과 보급으로 인해 점차 무선 개인정보 단말기들에 대한 피해도 늘어날 전망이다. WPKI(무선 공개키기반구조)나 PDA용 무선 VPN(가상사설망) 솔루션 등의 다양한 솔루션들이 속속 개발되고 있지만[7], 아직까지 이러한 개인 정보 기기들을 위한 보안은 연구단계에 불과하여 많은 피해가 예상되고 있으며 계속해서 늘어날 것으로 보인다.

3. 보안 솔루션

3.1 네트워크 보안 솔루션

위험을 사전에 방지하기 위해 대부분의 공공기관, 기업들이 네트워크를 위한 보안대책 마련 방안의 하나로 설치되고 있는 대표적인 네트워크 보안 솔루션은 방화벽, IDS, VPN 등이 있다. 허나 이러한 몇 개의 제품들만을 설치했다고 해서 안전하다고 할 수 없으며 취약한 여러 요인들의 제거를 위한 다양한 솔루션들이 설치되는 등 보안 솔루션의 다각화 시대가 열리고 있다.

3.1.1 침입차단 시스템(방화벽)

침입차단 시스템은 가장 널리 설치되어 사용되고 있는 대표적인 보안장비제품으로 외부망에서 내부망으로의 비인가자 침입을 차단시켜 주는 소프트웨어 혹은 하드웨어를 지칭한다. 방화벽은 접근제어 목록(Access Control List : ACL)에 따라 내부 네트워크의 자원들의 보호를 담당하고 있는 솔루션이다.

운용되는 프로토콜 계층의 위치에 따라서 크게 네트워크 계층에서 동작하는 시스템과 응용계층에서 동작하는 시스템 두 가지로 크게 구분되고 있으며, 구현 방식에 따라서 패킷 필터링, 애플리케이션 프록시, 서킷레벨 프록시, 상태검사 기법 네 가지로 구분된다. 각각의 기술들은 독자적으로 사용되기보다는 속도가 빠른 패킷 필터링과 패킷을 응용계층에서 세밀하게 차단 정책을 적용시킬 수 있는 애플리케이션 프록시 기술을 함께 사용하고 있으며, 최근에는 여기에 상태검사 기법을 대분분의 제품에서 적용하고 있다. 상태검사기법은 세계적으로 가장 널리 알려진 방화벽 업체인 체크 포인트사에서 특허 출원한 기

술로 세션의 연결정보를 분석해서 침입차단에 이용하는 기술이다.

3.1.2 침입탐지 시스템(IDS)

각각의 패킷에 대한 분석을 할 수 없는 침입차단 시스템인 방화벽과는 달리 침입탐지 시스템은 네트워크 패킷을 분석하고 이러한 패킷 중 해킹의 징후를 띠고 있는 것을 발견할 경우 관리자에게 경보 메일 송신, 공격 세부사항 로깅 또는 접속 단절 등 여러 다양한 대응 옵션을 제공하며 대부분의 침입과 공격을 탐지할 수 있는 시스템이다.

그러나 대부분이 패턴에 일치되는 경우의 탐지가 주를 이루고 있으며 이를 벗어난 경우 탐지가 어려운 단점이 있다. 최근 국내에서는 이러한 공격패턴 기반의 네트워크 침입탐지의 한계를 지적한 침입방지 시스템의 출현으로 업체간에 침입탐지 시스템과의 비교 논쟁이 있기도 하였다.

침입탐지 시스템은 패킷의 내용을 분석하고 이것이 침입인지를 결정하기 위해 저장된 공격패턴과 비교 분석하여야 하기 때문에 여기에서 많은 부하가 발생한다. 이를 해결하기 위한 다양한 노력들이 이루어지고 있으며, 고속의 장비와 4계층 스위칭 장비를 이용한 로드 밸런싱 장비를 이용해서 해결하고 있으며, 침입탐지 시스템은 단독으로 설치 사용하기보다는 침입차단 시스템이나 타 보안 시스템들과 연계해서 사용하여야 효과를 볼 수 있다. 이를 반영하듯이 많은 침입탐지 솔루션들이 침입차단 시스템과 상호연동이 가능하다. 새로 개발되고 있는 차세대 침입탐지 솔루션들은 브리지 모드로 동작될 수 있으며 침입탐지와 차단 기능을 동시에 지원 가능하도록 개발되고 있다.

3.1.3 안티 바이러스(Anti-Virus)

컴퓨터 바이러스는 초창기 감염된 파일이 다양한 경로를 거쳐 컴퓨터에 복사된 후 감염 파일의 실행으로 인해 다른 파일에 감염되거나 시스템을 손상시키는 형태로 존재했으나 네트워크의 확산과 기술의 발전으로 다른 해킹 수법들과 마찬가지로 많은 변화를 가져왔다.

컴퓨터 바이러스는 운영체제와 관계없이 네트워크를 통한 다운로드, 웹다운, 응용 프로그램의 실행, 메일 전송 등의 다양한 수단을 통해 급속한 속도로 전세계의 컴퓨터 시스템을 마비시킬 수 있다. 대부분이 매크로 형태의 바이러스로 최근의 컴퓨터 바이러스는 웜과 트로이 목마의 기능을 복합한 복잡하고 지능적인 특징을 갖는 형태로 출현하고 있다. 또 무선 인터넷을 통한 형태의 바이러스 전파가 새롭게 나타나 많은 피해가 우려되고 있다. 메신저 프로그램을 통해 전파되거나, WAP 바이러스, 무선 단말기 자체에 상주하거나, 스스로 감염할 목표물을 찾아가는 스텔스 바이러스, 하드웨어에 들어가는 칩 내부에서 작동하는 바이러스 등 다양한 형태의 출현이 예상되고 있으며, 향후 무선 정보 단말기의 보급에 따라 가장 큰 보안 위협으로 떠오르게 될 것으로 보인다.

3.2 통합 보안 솔루션

보안 감사를 통해 시도된 해킹 공격을 분석한 결과 90% 이상이 잘못된 보안 설정과 그를 사용하고 있는 소프트웨어의 지속적인 업그레이드 및 패치를 하고 있지 않은 것으로 조사되었다. 보안상의 헛점이 잘못된 관리에 있다는 것을 알 수 있다. 보안정책은 기업의 비즈니스 특성에 맞게 구체적으로 만들어야 하지만 외부정책을 그대로 인용해 사용하는 오류를 범하는 경우가 적지 않으며 대부분 해킹 사고의 원인은 보안 담당자가 보안 솔루션의 설정을 지속적으로 변경해 주어야 함에도 불구하고 이를 원활하게 관리하지 못하는데 있다. 즉, 해킹 방법은 날마다 지능적으로 변화하고 있는데, 방화벽이나 IDS는 구축 초기의

설정을 그대로 유지하고 있다는 것이다.

갈수록 늘어나는 보안 장비와 다양한 수법들에 대처하기 위한 장비 관리의 어려움과 전문 인력의 부재로 보안 장비가 설치되어 있어도 외부로부터의 침입에 적절하게 대응을 하지 못하는 경우가 많다. 이를 위해 설치된 보안 장비들을 관리하기 쉽고 운용을 간단하게 하려는 노력들이 진행되고 있다. 다른 한편으로는 보안관리를 전문으로 하는 아웃소싱형태의 업체들이 생겨난 것이 그 예라고 볼 수 있다. 그리고 한 가지 솔루션만이 독자적으로 설치되어 운용되는 것이 아니라 각 보안장비들을 통합해서 취약점을 보완한 형태의 통합 솔루션들과 관리 솔루션들이 개발 출시되고 있다. 대표적인 것으로는 보안장비들을 중앙에서 감시하고 로그들을 분석해서 현재 상태를 감시할 수 있는 통합보안관리 시스템(ESM)과 인증과 접근제어를 연계한 통합인증 및 권한관리를 들 수 있다.

3.2.1 ESM

ESM은 좁은 의미에서는 침입차단 시스템, 침입탐지 시스템, 안티 바이러스 등과 같은 단위 보

〈표 1〉 정보보안 체계별 솔루션 전략

중점 보안 대상	위험 요소	보 안 대 책	해당 솔루션
데이터, DB, 응용 시스템 보안	• 부적절한 데이터 입력 • 부당한 파일 사용 • 데이터의 도용 • 데이터의 변조 및 파괴 • 부당한 데이터 유출	• 파일 시스템에 대한 보안강화 • 비권한자의 데이터 접근 통제 • 업무구분을 통한 권한 지정 • DBMS 고유의 보안 기능 활용 극대화	• 로깅 시스템 • Auditing • DB 보안 • App 보안 • 접근제어 • PKI • DRM • 통합인증/권한관리(EAM)
주전산기 (서버)	• 시스템 다운 • 비인가자 서버 접속 • 비권한자의 자원 사용 • 내/외부인의 해킹 • 시스템 서비스의 거부 • 시스템 취약점 방치	• 사용자 계정 및 비밀번호의 관리 대책 설정(보안정책 설정) • 올바른 시스템 구성 및 지속적인 패치 적용 • 시스템 LOG 분석 및 감사 및 접근 통제 • 주기적인 보안진단 및 보완 • COPS(공개보안 진단툴) 설치, 운영	• 서버 보안 • 로깅 시스템 • Auditing • 접근제어 • 서버 취약점 분석
네트워크	• 외부 해커에 의한 접근 • SYN Flooding에 의한 서버의 Busy 상태 유발 • IP 스푸핑, 스니핑 • 네트워크 자원 접근	• 방화벽 운영 및 통제 정책 • 특정 패킷에 대한 필터링 • TCP Wrapper 설치, 운영 • 중요 데이터 암호화 전송 • 불필요한 데몬/서비스 제거	• 네트워크 접근 제어 • 네트워크 침입 차단 • 네트워크 침입탐지 • IP 주소 통제 시스템 • 네트워크 취약점 분석 • 네트워크 취약점 점검
개인 PC	• 비인가자의 접근 • 자료유출 • CMOS Password 비설정 • 바이러스 감염	• 화면보호기 기동 및 비밀번호 설정 • 파일 공유시 비밀번호 설정 • 백신 프로그램의 설치 운영 • CMOS 패스워드 설정	• PC 보안 • Anti-Virus
전산센터 시 설 물	• 비인가자의 전산실 출입 • 정전, 습도, 기온에 의한 시스템 정지 • 천재지변의 발생	• 비인가자의 전산실 출입통제 및 기록, 추적 • 무중단 전원 공급 장치(UPS), 항온, 항습기 설치 • 부대시설 정기점검 실시	• CCTV • 지문인식 • 생체인식

안 솔루션들로부터 전송되는 로그 데이터들을 관리하고 분석하는 관리 도구라고 할 수 있다. 반면 넓은 의미의 ESM이란 이러한 보안관련 데이터 분석이나 관리영역을 넘어 보안관리 영역 내에 산재되어 있는 잠재된 위험요소들을 사전에 제거하여 능동적으로 기업의 정보자산을 안전하게 지키는 데 중점을 두고 있는 종합적인 위험관리 도구라고 할 수 있다. 기존의 제품들은 단순히 로그를 통합해서 분석하는 정도의 기능으로 보안 솔루션들을 중앙에서 관제하는 역할을 수행하고 있으나, 최근 들어서는 보안 솔루션들이 점점 더 복잡해지고 정교해지고 있기 때문에 단순한 통합관리 차원을 넘어서 잠재적으로 산재해 있는 위험요소를 지속적으로 관리하고 예방하는 위험관리 차원에 초점을 두고 있는 제품들도 개발되고 있다[3, 7].

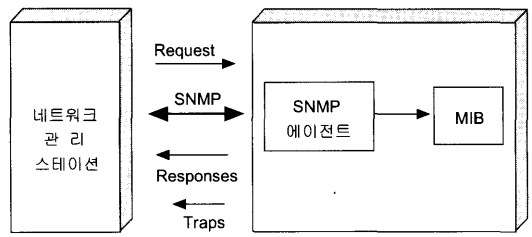
3.2.2 EAM

EAM은 ID와 패스워드의 관리 방안으로 나온 싱글 사인 온(single sign on)에 사용자의 지급과 담당 업무 등의 권한에 따라 시스템의 접근을 제어하는 기능을 추가함으로써 사용자와 관리자의 편의를 향상시키고 서로 다른 플랫폼이나 운영시스템, 웹서버, 애플리케이션간의 사용자 권한을 중앙에서 모니터링하고 제어하는 통합인증관리용 시스템이자 솔루션으로 이해할 수 있다. 한 번의 아이디 입력으로 다양한 시스템에 접근하고 각각의 ID에 따라 사용권한을 차등 부여한다. 싱글 사인온 기능에 사용자 통합관리, 다양한 인증방법지원, 사용자 관리용 디렉터리 서비스와의 통합 등의 기능을 갖춰야 한다.

4. MIB 기반 보안관리 시스템 모델

4.1 NMS

NMS 시스템은 인터넷을 구성하는 시스템들을 하나의 확고한 체계 내에서 관리하는 것을 말한다. TCP/IP 인터네트의 네트워크 관리는 네트워크 관리 스테이션들이 네트워크 요소들에게 관리 정보를 질의하는 분산 모델이라고 정의할 수 있다. 네트워크 요소에는 호스트, 라우터, X 터미널 서버 등 TCP/IP 프로토콜을 수행하는 것은 무엇이든 포함될 수 있으며, 이러한 네트워크 요소를 에이전트(Agent) 또는 피관리 시스템이라고 한다. (그림 1)는 TCP/IP 인터넷 관리 모델을 네트워크 레벨에서 그리고 한 쌍의 관리 스테이션과 에이전트 레벨에서 살펴본 것이다.



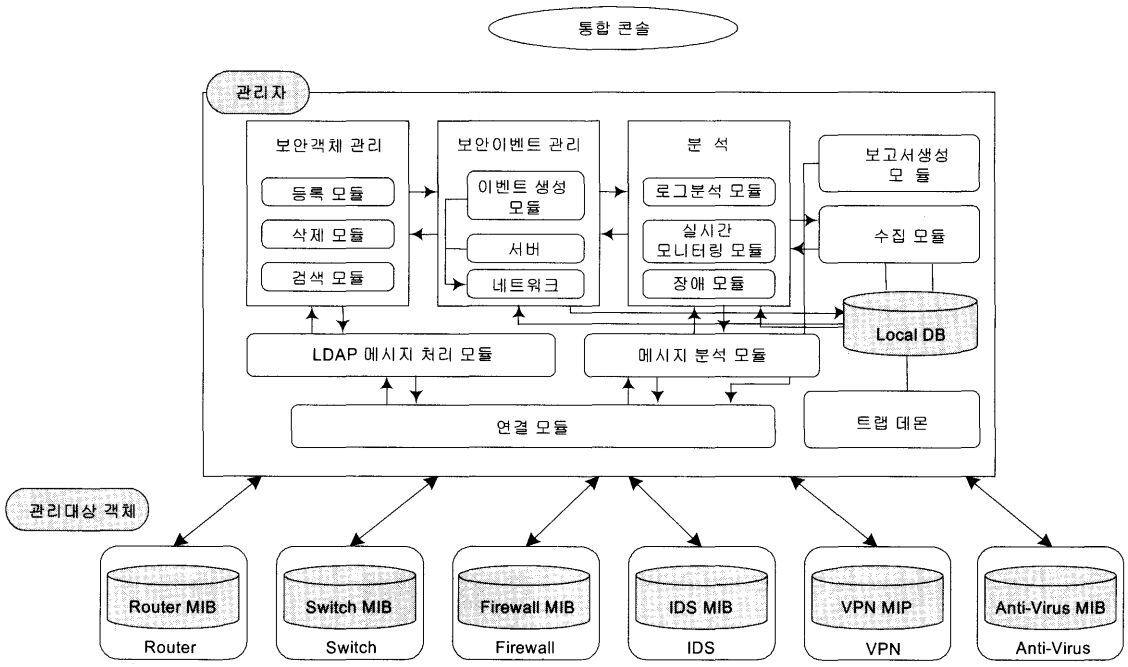
(그림 1) 관리 스테이션과 에이전트간의 질의 응답

네트워크 관리는 다음의 세 가지 요소로써 이루어진다.

1) MIB(Management Information Base)
   네트워크 요소들이 유지하는 값들을 나타낸다.
2) SMI(Struct of Management Information)
   MIB 내에 저장되어 있는 변수들을 참조하기 위해서 사용되는 공통 구조와 식별 기법의 집합을 말한다.
3) SNMP(Simple Network Management Protocol)
   관리자 스테이션과 네트워크 요소간의 통신을 수행하기 위해서 사용하는 프로토콜이다.

4.2 MIB 기반의 시스템 관리

MIB 기반의 시스템은 보안적 네트워크 장비 또는 프로세서에 대한 MIB을 정의하고 이 정보를 받아 네트워크 현황을 파악한다. (그림 2)은 MIB 기반의 시스템의 구조를 나타내고 있다. (그림 2)



(그림 2) NMS-based Security Management 시스템의 구조

에서 인터넷 관리 모델을 관리자 시스템과 보안 관리 중심의 관리 대상 객체로 구분하였다. 보안 관리 대상 객체는 앞 절에서 기술한 라우터, 스위치, 방화벽, 침입탐지 시스템, VPN, Anti-virus 등이 MIB 형태로 존재하게 되며, 관리자 시스템은 이러한 다양한 종류의 MIB 정보를 요청, 수집, 분석, 관리하는 모듈이 필요하게 된다.

5. 결 론

해킹 등 네트워크에 대한 침해는 점차로 지능화되고 악성화 되고 있으며 다양한 기술들이 결합된 형태로 진화하고 있다. 다시 말해 단순한 보안 정책과 단일 보안 솔루션으로는 지능적 네트워크 침해에 대해 대처하기가 역부족이라는 의미이며, 이에 본 논문에서는 NMS-based Security Management를 이용하는 방안을 제안하였다. 이를 위해 SNMP를 이용하여 네트워크 장비를 제어하였고, 네트워크 보안과 관련하여 SNMP 자체의 보안 개념을 사용하는 것은 물론 MIB의 확장을 그 배경으로 삼았다. 현재 네트워킹 장비에서 보안 기능이 핵심 요소로 자리잡아 가고 있으며, 단순 예방과 탐지만으로는 갈수록 늘어나는 침해사고에 대처하기는 어려워지고 있다. 그래서 네트워크를 탐지하고 직접 네트워크 장비를 조작하여 보안 레벨을 높이는 NMS-based 형태의 보안 솔루션은 앞으로 더욱 주목을 받을 것으로 예상된다.

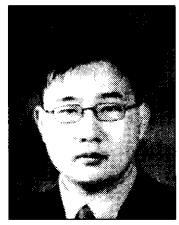
참 고 문 헌

[1] Warwick Ford, "Computer Communications Security", PTR Prentice Hall, Englewood Cliffs, New Jersey.

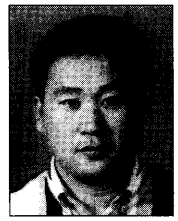
[2] E. Ammroso, "Intrusion Detection : An Introduction to Internet Surveillance, Correlation, Traps, Trace Back, and Response", Intrusion. Net Books, 1999.

[3] J. P. Anderson. "Computer security threat monitoring and surveilance", Technical report, James P. Anderson Company, Fort Washington, Pennsylvania, April 1980.
[4] D. Clark and J. Wroclawski, "An Approach to Service Allocation in the Internet", IETF Internet Draft, July 1997.
[5] R. Braden, et. al., "Resource ReSerVation Protocol (RSVP) : Version 1 : Functional Specification", IETF RFC 2205, September 1997.
[6] J. Anderson, S. Brand, L. Gong, T.Haigh, S. Lipner, T. Lunt, R.Nelson, W. Neugent, H. O. Roam, M. Ranum, R. Schell, and E. Spafford. "Firewalls : An Expert Roundtable", IEEE Software, 12(5), pp.60-66, 1997.
[7] Y. Bartal, A. Mayer, K. Nissim and A. Wool, "Firmato : A Novel Firewall Management Toolkit", IEEE Symposium on Security and Privacy, pp.7-31, 1999.
[8] J. Chomicki, J. Lobo and S. Naqvi. "Axiomatic conflict resolution in policy management", Technical Report ITD-99-36448R, Bell Labs, February 1999.

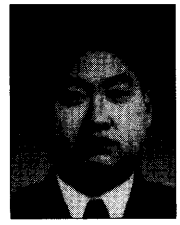
구 자 환
성균관대학교 공학석사
현재, 성균관대학교 박사과정
LG CNS 정보기술연구소 연구원



박 병 연
대전산업대학교
공주대학교 교육정보대학원
KIST/시스템공학연구소 입사
한국전자통신연구원
한국과학기술정보연구원



유 기 성
성균관대학교 과학기술대학원
KIST/시스템공학연구소 입사
한국전자통신연구원
한국과학기술정보연구원



이 행 곤
전북대학교
전산통계학과 이학석사
전북대학교 시간강의
ICU 강사
한국과학기술정보연구원 입사

엄 영 익
서울대학교 이학사
서울대학교 이학석사
서울대학교 이학박사
성균관대학교 교수
한국전자통신연구원 초빙연구원
미국 Univ. of California, Irvine 방문교수