비정상 패킷 대응시스템의 설계 및 구현

°김용배, °최병선, °이성현, °이원구, °이재광
°한남대학교 컴퓨터공학과 컴퓨터네트워크실험실
e-mail:ybkimb@lgchem.co.kr,
{bschoi, shlee, wglee, jklee}@netwk.hannam.ac.kr

Applying Design and Implementation of Response System Against Abnormal Packet

°Yong-Bae Kim, °Byoung-Son Choi, °Seoung Hyeon Lee,
°Won-Goo Lee, °Jae-Kwang Lee
°Dept of Computer Engineering, Hannam University

요 약

최근 컴퓨터 기술의 발달과 인터넷의 발전으로 인해 업무 효율이 높아졌고 생활의 질이 높아졌다. 하지만 컴퓨터 기술과 인터넷 기술의 발전은 긍정적인 효과뿐만 아니라 외부 시스템의 불법 침입, 중요 정보의 유출, 서비스 거부 공격 등 역기능도 생겨났다. 이러한 사이버 공격에 대한 능동적으로 대응할 수 있는 기술이 요구되는데 능동적인 대응의 가장 기본적으로 요구되는 기술이 공격자의 실제 위치를 파악하는 역추적 기술이라고 할 수 있다. 이에 본 논문에서는 분산 서비스 거부 공격에 대하여 효율적으로 역추적 하기 위해서 액티브 네트워크 기반의 역추적 시스템을 분석 및 설계한다.

1. 서론

비정상적인 Packet에 의한 Denial of Service(DoS) 공격은 최근 및 년 동안 인터넷에 행하여져 왔으며 대표적으로 2001년 8월 "Code Red" Worm 9월 "Nimda" Worm, 2002년 6월 Denial-of-Service Vulnerability in ISC BIND 9 .10월 "Apache/mod_ssl " Worm 2003년 1월 "MS SQL Server" Worm 등이 국내 네트워크 자원을 소모하는 공격형태이다. 인터넷은 중요한 통신기반 시설로서 또는 전자상거래를 통한 이유의 문제에 있어서 중요도와 의존도가 높아가고 있으며 이러한 상태의 서비스 공격에 의한인터넷 중단의 문제는 매우 중요한 문제로 대두되고 있다. 그러나, 서비스 거부공격으로부터 자신의 사이트를 보호하고 대응할 수 있는 확실한 해결책이 없는 상황이다[1][2].

본 논문에서는 대형 네트워크에서 네트워크 관리 시스템(NMS)을 통하여 실제 네트워크에서 발생되는 바이러스 및 서비스 거부 공격(DoS) 트래픽의 이상 흐름을 통해 비정상적인 패킷형태가 어떻게 나타나는지 분석하고 그 특성에 관하여 연구하고자 한다. 그리고, 서비스 거부 공격(DoS)의 이상현상을 최소화하기 위하여 보안시스템의 효율적인 배치와 운영방법 연구를 통하여 안정적이고 효율적인 네트워크 관리의 대안을 제시하고자 한다.

2. 관련연구

네트워크 관리란 신산 네트워크가 지속적이고 효율적으로 광범위한 지역에서의 정보교환, 자원공유, 지명적인 고장의 대체가능, 유연성 있는 작업 환경 제공과 같은 복잡해진 기능을 수행하고 보다 향상된 서비스를 제공할 수 있도록 신산 네트워크에 연결된 장비와 호스트간의 트래픽에 대한 모니터링을 통해 서비스의 중단없이 효율적으로 통신 네트워크를 운용할 수 있도록 네트워크 자원의 감시 및 보고와 필요한 경우 제어를 수행하는 제반 활동을 의미한다[1][6].

2.1 네트워크 관리

2.1.1 MIB(Management Information Base)

MIB는 SNMP에서 관리하는 정보의 데이터베이스와 같은 것으로 (관리 항목의 정의와일 및 표 등이 있는 것), 어떤 항목에 대하여 문의하면 어떤 대답이 되돌아올지를 각각 정해놓고 있다. MIB에는 다음의 세 종류가 있다[3].

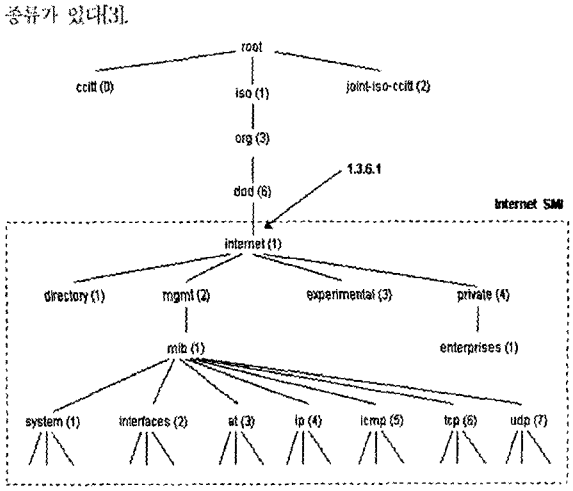

그림 1. MIB구조

MIB의 오브젝트는 ASN.1이라는 추상 구문 표기법에 의해 정의 ·

※ 본 연구는 산업자원부의 지역혁신 인력양성사업의 연구결과로 수행되었음.