[5A-22]

침입 대응을 위한 ICMP 기반의 IP 역추적 시스템 분석 및 설계

최병선*, 이원구*, 이재광*
*한남대학교 컴퓨터공학과 컴퓨터네트워크실험실
e-mail:{bschoi, wglee, jklee}@netwk.hannam.ac.kr

The Design and Implementation of ICMP-based IP Traceback System for Intrusion Response

Byoung-Son Choi*, Won-Goo Lee*, Jae-Kwang Lee*
*Dept of Computer Engineering, Hannam University

요 약

최근 인터넷의 급속한 보급 확대 및 대중화에 따라 네트워크상의 서비스 속도와 정보보안은 인터넷 사용자에게 중요한 문제로 대두되고 있고, 이로 인해 네트워크의 트래픽 증가와 공격자로부터의 공격이 점점 증가하고 있는 현실이다. 인터넷 사용자의 급속한 증가로 인한 복잡한 TCP 반응과 연관되어 네트워크 서비스에 많은 패킷 손실을 야기하게 되었다. 이러한 문제를 해결하기 위하여 대학 연구소와 기업체에서는 침입대응 시스템을 개발하게 되었고, 공격자의 근원지를 추적하는 역추적 시스템이 등장하게 되었다. 따라서 본 논문에서는 능동적인 해킹 방어를 위한 역추적 시스템을 분석하고, 리눅스 기반의 역추적 시스템을 설계하였다.

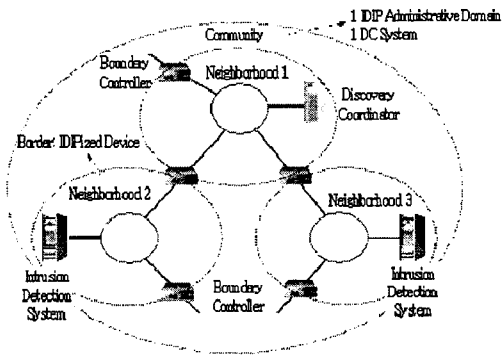
1. 서론

컴퓨터와 네트워크의 보급이 일반화되면서, 현재 인터넷으로부터 기업이나 국가 조직 내부의 정보나 자원을 보호하기 위해 여러 가지 정보보호시스템을 비롯한 보안 네트워크를 구성하여 네트워크 및 시스템을 운영하고 있다. 그러나 기존의 침입 차단 시스템과 침입 탐지 시스템과 같은 시스템 외부방어 개념의 보안 대책은 전산망 내의 중요한 정보 및 자원을 보호함에 있어서 그 한계를 갖는다. 인터넷 사용자의 급증에 따라, 인터넷을 통한 다양한 해킹 및 불순한 의도를 지닌 공격에 의한 침해사고 역시 크게 증가되고 있다. 이러한 해킹의 피해로부터 네트워크 시스템 및 서버를 보호하기 위해 각종 보안 강화 시스템이 개발되어 운용되고 있으나, 현재 사용 중인 보안강화 도구들은 수동적인 방어 위주로 공격자의 해킹 시도 자체를 제한하는 것이 아니라 해킹이 시도된 후 대처하는 제약 등으로 해킹 자체를 방지하는 데는 한계를 가지고 있다. 능동적인 해킹 방어를 위한 가장 기본적인 기술은 해커의 실제 위치를 추적하는 역추적 시스템이라 할 수 있다[1]. 본 논문에서는 해킹으로 판단되는 침입에 대하여 라우터의 구조적 변경 없이 효율적으로 역추적 하기 위해서 ICMP 역추적 메시지(ICMP Traceback Message)를 이용한 ICMP 기반의 역추적 시스템을 설계한다. ICMP 역추적 메시지의 생성은 라우터를 포트 미러링하는 "역추적 Agent"가 담당하며, 이 메시지를 수신하는 피해 시스템은 해당 메시지를 저장하고, "역추적 Manager"가 DDoS류 공격을 탐지하게 되면 해당 메시지 정보를 이용하여 역추적을 시작하여 공격자의 근원지를 찾아내고, 이를 통하여 침입대한 대응을 시도할 수 있게 된다.

2. 관련연구

2.1 IDIP(Intruder Detection and Isolation Protocol) 분석

IDIP는 침입탐지 시스템, 방화벽, 호스트, 보안관리 관련 요소 시스템들간의 협력 작업하기 위한 프로토콜을 포함한 보안 기반 구조(infrastructure)이다[2][3].



[그림 1] IDIP에서 네트워크 구조

※ 본 연구는 산업자원부의 지역혁신 인력양성사업의 연구결과로 수행되었음.