비정상 트래픽 상황에서 효율적 침입 탐지 시스템(EIDS) 구조 연구

*권영재, 이두만, 임홍빈, 정재일
한양대학교 전자통신컴퓨터공학과
e-mail : {brainreal, blueldm, hbyim}@mnlab.hanyang.ac.kr, jijung@hanyang.ac.kr

An Architecture for Efficient Intrusion Detection System of Abnormal Traffic

*Young-Jae Kwon, Du-Man Lee, Hong-bin Yim, Jae-Il Jung
Division of Electrical and Computer Engineering
Hanyang University

Abstract

Intrusion detection technology is highlighted in order to establish a safe information-oriented environment. Intrusion detection system can be categorized into anomaly detection and misuse detection according to intrusion detection pattern.

In this paper, we propose an architecture to make up for the defect of conventional anomaly intrusion detection. This architecture reduces additional resource consumption and cost by placing the agent in the strategic location in Internet.

I. 서론

현대인들의 생활환경에서 인터넷은 중요한 부분을 차지하고 있으며, 사용자의 수도 급증하고 있는 추세이다. 인터넷상의 다양한 호스트로부터 전달되는 개인 프라이버시 정보는 네트워크 공격에 무방비로 노출될 위험이 매우 높으며, 이에 대한 대응책이 절실하게 요구 되고 있다.

현재 네트워크상의 여러 가지 위협들로부터 시스템을 보호하기 위한 보안 제품들로 침입차단시스템, 침입탐지시스템, 바이러스 툴, VPN(Virtual Private Network) 등이 있으며, 특히 침입탐지 기술은 안전한 정보화 환경을 구축하는데 주목받는 기술로 부각되고 있다.[1]

본 논문에서는 기존의 이상 침입 탐지의 단점인 False Positive 오판 문제와 오용 침입탐지의 단점인 False Negative 오판 문제를 보완하고 에이전트를 인터넷상에서 전략적인 위치에 배치하여 추가적인 리소스와 비용을 줄일 수 있는 구조를 제안한다.

II. 본론

기존의 침입탐지시스템은 중앙 시스템 자체가 침입의 대상이 될 수 있고, 감사 대상이 제한적일 수밖에 없다. 또한 수행중인 침입탐지시스템의 설정내용을 변경하거나 기능을 추가/변경하기 위해서는 시스템 전체를 재시작 해야 하며 침입자가 침입탐지시스템을 공격할 경우, 침입탐지시스템의 서비스가 중단되거나 오류가 일어나는 등의 문제점이 발생할 수 있다.[2]

또한 기존 침입탐지시스템의 단점을 보완한 분산 침입탐지시스템의 경우에는 다수의 침입탐지시스템을 설치, 운영해야하므로 배치의 어려움뿐만 아니라 네트워크 자원 부하를 증가시키는 단점을 갖는다.[3]

따라서 본 논문에서는 효율적인 침입탐지시스템을 구축하기 위하여 분산된 에이전트 구조를 통해 탐지 효율을 높이고 각 에이전트들은 수집한 정보를 간단하게 정리하여 매니저로 전달함으로써 침입탐지시스템이 특정

부분에서 공격받는 경우라도 다른 에이전트의 감사 데이터들과의 통계를 통해 문제를 발견할 수 있는 구조를 제안한다.

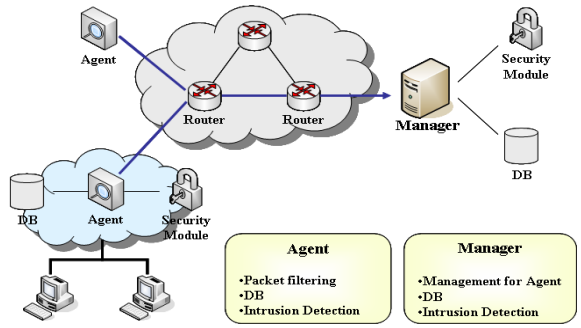

그림 1 EIDS 구조

에이전트(Agent)는 특정 호스트에서 동작하는 침입탐지 시스템으로, 플랫폼에 독립적이므로 이 기종 간에 에이전트 구성이 가능하고, 주어진 에이전트의 성격에 따라 필요한 클래스만으로 구성이 가능하다. 에이전트는 노드들의 자원과 비용을 줄이기 위해 클러스터링을 하여 최적화된 배치를 한다. 매니저(Manager)는 에이전트에서 얻어지는 정보를 바탕으로, 에이전트에서 탐지하지 못한 침입을 탐지할 수 있다. 에이전트에서는 이상침입탐지를 수행하고, 매니저에서는 오용침입탐지를 수행한다.

특정노드에 에이전트를 구현하는 것은 추가적인 리소스와 비용이 요구되므로 전략적인 위치에 배치되어야 한다. 반면에 그 수는 충분해야 하고, 노드들 사이에 적절히 분산되어 있어야 한다. 이를 위해 EIDS 최적 배치 Algorithm을 제안하여 효율성을 높이도록 한다.

Ⅲ. 실험평가

EIDS의 성능 분석을 위하여 다양한 공격 유형을 적용시킴으로써 각각의 탐지율, False Positive 오판율, False Negative 오판율을 측정하였다.

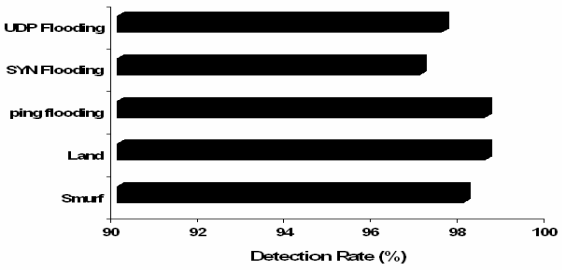

그림 2 공격 유형에 따른 탐지율

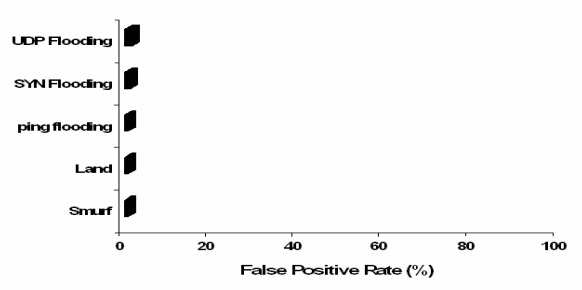

그림 3 공격 유형에 따른 False Positive 오판율

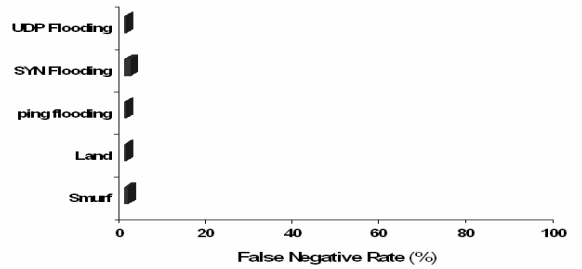

그림 4 공격 유형에 따른 False Negative 오판율

Ⅳ. 결론 및 향후 연구 방향

본 논문에서 제안한 구조는 기존의 이상침입탐지의 단점인 False Positive 문제와 오용침입탐지의 단점인 False Negative 문제를 보완하고 에이전트는 인터넷 상에서 전략적인 위치에 배치하여 추가적인 리소스와 비용을 줄일 수 있다.

향후 에지 라우터에 에이전트를 설치하여 실제 망 환경에서의 적용이 요구되며, 에이전트와 매니저의 구조를 이용한 최적배치 알고리즘의 최적화가 요구된다.

참고문헌

[1] 조휘갑, “차세대 네트워크 보안 기술”, 한국정보보호진흥원, 2002년 11월.

[2] 최주영, 최은정, 김명주, "대규모 네트워크 상의 다중공격에 대비한 분산 침입탐지시스템의 설계 및 구현", 한국사이버테러정보전학회논문지:정보보증논문지 , 1598-7329 , 제1권1호 , pp.21-29 , 2001.

[3] Eugene H. Spafford, Diego Zamboni, "Intrusion detection using autonomous agents", Computer Networks, pp. 547-570, 2000.

[4] Denning, D.An "Intrusion Detection Model", IEEE Transactions on Software Engineering, vol SE-13, no.2, 1987.