2000년 한국정보처리학회 추계 학술발표논문집 제7권 제2호

SNMP와 이동 에이전트 기반의 침입탐지 시스템 설계

강정민*, 이형효*, 이동익*, 윤석환**
*광주과학기술원 정보통신공학과
jmkang@geguri.kjist.ac.kr
{hlee, dilee}@kjist.ac.kr
**정보통신연구진흥원

A Design of Intrusion Detection System based on SNMP and Mobile Agents

Jung-Min Kang*, Hyung-hyo Lee*, Dong-Ik Lee*, Seok-Hwan Yoon**
*Department of Infomation and Communication, K-JIST
**Institute of Information Technology Accessment

요약

본 논문에서는 대규모 네트워크 환경에서의 분산된 침입탐지 시스템(Intrusion Detection System:IDS)을 망관리의 표준 프로토콜인 SNMP(Simple Network Management Protocol)와 이동 에이전트를 이용해서 진보된 형태의 다중호스트/네트워크 기반의 침입탐지 시스템 프레임워크를 제시하였다. SNMP 에이전트는 호스트 기반의 침입탐지를 수행하며 분산된 호스트들에서의 이동 에이전트는 플랫폼 독립적인 네트워크 기반의 침입탐지를 함으로써 시스템의 유연한 확장성, 결함허용 및 시스템의 동적인 구성을 가능케한다.

1. 서론

정보통신 관련 기술의 급격한 발달 및 효율적인 정보교환과 처리를 위해 이전까지는 폐쇄 환경 내에서 교환되던 중요한 정보들이 정보시스템 내로 전이되었다. 이들 정보 시스템은 개방 구조를 갖는 통신망 상에서 동작하므로, 외부로 부터의 침입 및 내부 공격자에 의한 정보의 유출 위험에 항상 직면해 있다. 이런 위험에 대한 대처방안으로 대두된 침입탐지 시스템의 연구가 활발하게 진행중이다. 하지만 기존의 침입탐지 시스템은 확장성, 효율성 및 구성면에서 한계 및 단점을 지니고 있다[4]. 가장 일반적인 단점은 침입탐지를 위한 데이터 수집 및 분석작업이 시스템내의 하나의 개체를 중심으로 이루어진다는 점이다.

이런 문제에 대한 해결방법의 하나로서 새의 무리나 개미 떼 같은 집단이 상호협력을 통한 고도의 작업이 가능한 생물학적인 발상을 이동 에이전트에 적용하는 방법이 시도되고 있다.

본 논문에서는 대규모 네트워크 환경에서의 분산 침입탐지 시스템을 망관리의 표준 프로토콜인 SNMP와 이동 에이전트를 이용해서 진보된 형태의 다중호스트/네트워크 기반의 침입탐지 시스템 프레임워크를 제시하고자 한다.

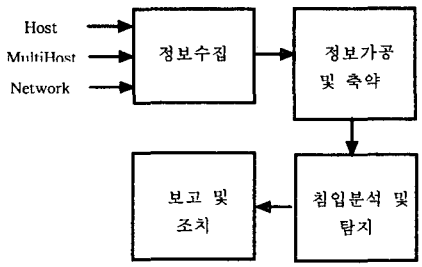
본 논문의 구성은 2장에서 기존의 침입탐지 시스템의 문제점 파악을 통해서 침입탐지 시스템이 지녀야 할 특성들을 살펴보고, 3장에서는 제안된 SNMP와 이동에이전트 기반의 침입탐지 시스템을 설계하고 각 구성요소들을 살펴본다. 4장에서는 제안된 시스템의 특성과 단점을 살펴보고 향후 연구과제를 기술한다.

2. 관련연구

침입탐지 시스템의 개념과 기존의 침입탐지 시스템들의 문제점들을 파악하고 침입탐지 시스템에서의 요구사항들을 고찰한다.

2.1 침입탐지 시스템

침입탐지란 크랙커 같은 권한이 없는 사용자의 컴퓨터 시스템 사용 뿐만아니라 내부 위협자들 처럼 합법적인 액세스를 했지만 그들의 권한을 오용, 남용하는 사람들을 식별하는 것이다. 여기서 침입이란 시스템 자원의 가용성(Availability), 비밀성(Confidentiality), 무결성(Integrity)를 저해하는 행위들의 집합을 일컫는다[1].



(그림 1) 침입탐지 시스템의 수행과정

침입탐지 시스템의 일반적인 수행과정을 살펴보면 정보수집(Data Collection), 정보가공 및 축약(Data Reduction), 침입 분석 및 탐지(Analysis and Detection), 보고 및 조치(Report and Response)로서 이루어 진다.

여기서 정보수집 즉 데이터 소스에 의한 침입탐지 시스템을 분류하면 일반적으로 호스트 기반의 침입탐지 시스템과 네트워크 기반의 침입탐지 시스템으로 분류할 수 있다. 호스트 기반의 침입탐지 시스템은 하나의 시스템에서 감사자료를 수집하여 침입여부를 판단하는 시스템을 말하며, 네트워크 기반의 침입탐지 시스템은 호스트들의 연결된 네트워크내에서의 패킷정보에 의한 침입 여부를 판단하는 시스템이다. 그리고 다중 호스트 기반의 침입탐지 시스템과 호스트/네트워크 기반의 혼합 침입탐지 시스템같은 혼합된 형태의 시스템들도 존재한다.

본 논문에서는 호스트들에서의 침입 여부를 판단하는 SNMP 에이전트와 패킷감시을 위한 이동 에이전트를 둠으로써 진보된 형태의 다중호스트/네트워크 기반의 침입탐지 시스템 프레임워크를 제시하고자 한다.

2.2 기존 침입탐지 시스템의 단점

기존의 대부분의 호스트 기반, 네트워크 기반의 침입탐지 시스템은 오직 하나의 호스트에서 데이터를 수집하고 분석하는 중앙집중형 특징을 가진다. 분산된 데이터 수집을 하는 형태의 침입탐지 시스템 조차도 수집된 데이터의 분석을 위해서는 수집된 데이터가 중앙의 호스트로 이동된다. 이러한 접근방법들은 다음과 같은 단점들을 가지고 있다[4].

- 중앙집중 분석 시스템이 침입을 받으면 전체 네트워크가 위협을 받을 수 있다.
- 하나의 호스트에서 모든 데이터를 분석, 처리하는 것은 네트워크 규모의 확장성을 제한한다.
- 침입탐지 시스템의 재구성 및 기능추가가 어렵다.

2.3 침입탐지 시스템의 요구사항[3]

다음은 침입탐지 시스템들의 메커니즘에 상관없이 요구되는 특징들이다.

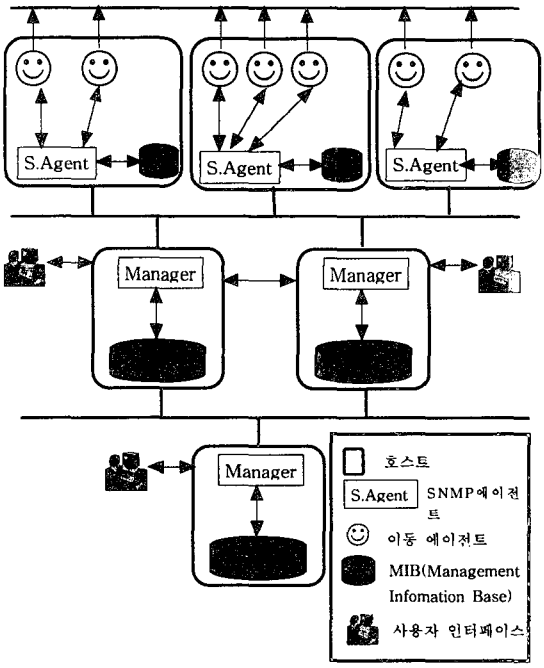
- 실행지속 : 최소한의 인적감독에 의한 실행을 지속해야 한다.
- 결함허용 : 시스템 파괴나 재초기화시 회복할 수 있는 기능을 지원해야 한다.
- 파괴저지 : 침입자에 의한 시스템의 변경시 자체적인 모니터와 탐지를 할 수 있어야 한다.
- 확장성 : 감시대상이 되는 호스트들의 증가시 그 호스트들을 모니터할 수 있어야 한다.
- 최소의 서비스 저하 : 침입탐지 시스템의 일부 구성요소가 작동불능시 나머지 구성요소들은 가능한한 적게 영향을 받아야 한다.
- 동적 재구성 : 시스템의 재시작없이 재구성할 수 있어야 한다.

3. SNMP,이동 에이전트 기반의 침입탐지 시스템

본 장에서는 비교적 단순한 기능을 가진 이동 에이전트들의 협조를 통해서 고도의 네트워크 침입탐지를 수행하고, SNMP 에이전트들은 분산된 각 호스들에서 호스트 기반의 침입탐지를 수행하는 통합된 침입탐지 시스템을 설계하고 기능을 살펴본다.

3.1 전체구조

제안된 본 시스템은 (그림2)와 같이 계층적인 구조를 가지며 필수적인 구성요소들로서는 이동 에이전트, SNMP 에이전트 그리고 Manager가 있다. 가장 하위레벨의 이동 에이전트들은 상호 협력적인 작업을 통해 패킷정보를 수집, 분석하는 자체적인 침입탐지를 수행한다.



(그림 2) SNMP, 이동 에이전트 기반의 IDS구조

한편 SNMP 에이전트는 호스트 기반의 침입탐지를 수행하며 탐지된 이상행위는 SNMP의 Trap메시를 통해 해당되는 Manager에게 보고한다. Manager는 능동적으로 GET(get-Next) 또는 SET 메시지를 통해서 분산된 호스트들을 탐지, 조치를 취할 수 있으며, 수동적으로 받아들인 Trap메시지에 대해서도 신속한 조치를 취할 수 있다.

3.2 구성요소

3.2.1 이동 에이전트

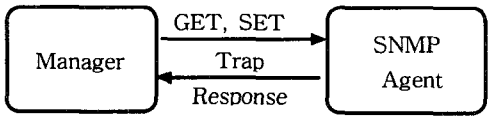
비교적 단순한 기능을 하는 이동 에이전트들의 상호협력을 통해서 데이터 수집 및 분석을 하는 고도의 네트워크 침입탐지를 하는 것이 이동 에이전트들의 역할이다. 예를 들어 이동 에이전트는 접근금지된 호스트에 대한 telnet연결을 시도하는 이상행위를 탐지하고 SNMP 에이전트 또는 Manager에게 보고할 수 있다.

에이전트들은 독립적으로 실행되는 개체들이기 때문에 IDS를 재시작할 필요없이 다른 구성요소들을 추가, 삭제할 수 있는 확장성과 자신들을 동적으로 재구성할 수 있는 메커니즘을 제공한다. 그리고 다수의 에이전트들이 상호협력을 위해서 그룹을 형성할 경우, 서로의 능력을 보완해준다는 이점 이외에 하나의 에이전트가 고장을 일으켜도 침입탐지 작업에 큰 지장을 초래하지 않는다는 장점이 있다. 그리고 분산된 호스트들이 다중 플랫폼이라는 것을 고려할 때 이식성과 플랫폼 독립성을 지원하는 이동 에이전트는 자체적으로 새로운 버전으로의 업그레이드가 가능하므로 효율성을 제공한다. 그외에 이동 에이전트들이 수행할 수 있는 기능들을 살펴보면 다음과 같다.

- 에이전트들은 유전자 프로그래밍 또는 다른 machine learning 기술을 이용해서 학습할 수 있고 진화할 수 있다.
- 에이전트들은 필요시 상호 협력을 위해서 호스트에서 호스트로 이동할 수 있다.
- 에이전트는 지역 호스트의 SNMP 에이전트간의 통신을 통해서 SNMP 에이전트가 제공하는 MIB정보를 접근하여 Manager에게 즉시 혹은 수집하여 나중에 전달할 수 있다.

3.2.2 SNMP 에이전트

분산된 각 호스트에서 데몬(daemon) 프로세스로서 수행하면서 호스트기반의 침입을 탐지한다. 그리고 Manager의 메시지에 대한 응답을 행하며 이상행위의 발견시 즉각적인 조치는 Trap메시지를 통해 능동적으로 관련된 Manager에게 보고한다.



(그림 3) SNMP의 기본통신

3.2.3 Manager : 침입탐지 분석 시스템

Manager는 제안된 시스템에서의 상위레벨 분석기로서 이동 에이전트와 SNMP 에이전트로부터 수집된 정보의 신속하고 정확한 분석을 통한 종합적인 침입의 판정을 수행한다. 이는 해당 결과에 대한 재분석을 수행함으로써 하위레벨에서의 침입판정에 대한 신뢰성을 부여함과 동시에 분산된 다중공격등에 대한 판정기능을 가짐으로써 보다 광범위한 정보의 분석과 감시를 제공한다. 예를 들어 false positive 또는 false negative같은 에러의 처리가 가능하다. 그리고 일부 Manager의 고장은 전체 시스템의 고장을 유발시키지 않는 결함허용을 제공하기도 한다. Manager사이에는 SNMPv3의 Inform메시지를 통해 상호협력적인 분석, 처리가 가능하다. 부가적으로

Manager는 사용자 인터페이스를 통해 전체 시스템의 접근지점을 제공한다.

3.2.4 사용자 인터페이스

사용자가 제안된 IDS와 상호작용하면서 제어할 수 있는 관리자 모드의 인터페이스 설계가 요구된다. Interactive한 접근을 위해서 GUI환경으로 구현될 수 있으며 유지측면에서의 command-line인터페이스로 구현될 수도 있다.

4. 결론 및 향후 연구과제

본 논문에서는 기존의 침입탐지 시스템에서의 가장 일반적인 단일 호스트위주의 중앙집중적 데이터 분석, 처리의 문제점을 해결하기 위해 SNMP 에이전트와 이동 에이전트를 이용한 다중 호스트 기반의 침입탐지 시스템 구조를 제시하였다. 그리고 2.3에서 기술한 침입탐지 시스템의 요구사항을 제안된 시스템의 이동 에이전트가 만족시키고 있음을 보였다.

향후 연구과제로는 서로 다른 사용자들에 대한 접근통제에 대한 메커니즘, 만약 두 개의 Manager가 같은 SNMP 에이전트를 제어하는 경우에 생기는 제어정보의 일관성유지를 위한 메커니즘과 설계된 아키텍쳐를 기반으로 프로토타입 개발과 침입탐지 성능분석에 대한 연구가 필요하다.

참고문헌

[1] B. Mukherjee, T.L. Herberlein, and K. N. Levitt, "Network intrusion detection" IEEE Network, 8(3):26-41, May/June 1994.

[2] M. Crosbie and G. Spafford, "Defending a computer system using autonomous agents" In Proceedings of the 18th National Information Systems Security Conference, Oct 1995.

[3] M. Crosbie and G. Spafford, "Active defense of a computer system using autonomous agents" Technical Report 95-008, COAST Group, Department of Computer Sciences, Purdue University, West Lafayette, IN47907-1398, Feb 1995.

[4] Jai Sundar Balasubramaniyan, Jose Omar Garcia-Fernandez, David Isacoff, Eugene Spafford and Die해 Zamboni, "An Architecture for Intrusion Detection using Autonomous Agents" COAST Group, Department of Computer Sciences, Purdue University, West Lafayette, 1998.

[5] D.E. Denning. "An Intrusion-Detection Model." IEEE Transactions on Software Engineering, 13(2):222-232, Feb 1987.

[6] S.Staniford-Chen et al. "Common Intrusion Detection Framework" WWW page at http://seclab.cs.ucdavis.edu/cidf/.

[7] Mani Subramanian, "Network Management - An introduction to principles and practice" Addison Wesley, 2000.

[8] David Zeltserman, "A Practical Guide to SNMPv3 and Network Management" Prentice Hall, 1999.

[9] Willian Stallings, "SNMP, SNMPv2 ,SNMPv3, and RMON 1 and 2" Addison Wesley,1999.

[10] 유정준, 백주성, 박종열, 이동익, "자바 기반 이동 에이전트 시스템: X-MAS", 한국정보처리학회 논문집, 1998.

[11] 유정준, 백주성, 박종열, 이동익, "이동 에이전트와 통신을 위한 에이전트 위치발견", 한국정보처리학회 논문집, 1998.

[12] 전병국, 김영철, "효율적인 통신망 관리를 위한 이동 에이전트 응용" 한국정보처리학회 춘계학술대회 논문집, 2000.

[13] 김병구, 김동수, 정태명, "계층적 구조를 갖는 침입탐지 통합 시스템 설계" 한국정보처리학회 추계학술대회 논문집, 1999.