침입탐지면역시스템모델 설계

김 강*, 이건익**, 전영철**
* 강원관광대학 관광정보처리과
** 관동대학교 컴퓨터학과
e-mail : kkang424@hanmail.net, lki@kd.ac.kr, totalic@kd.ac.kr

Design of Intrusion Detection Immune System Model

Kim Kang*. Lee Keon Ik**, Jeon Young Cheol**
* Dept of Tourism Information Process, Kangwon Tourism College
** Dept of Computer, Kwandong University

요 약

컴퓨터의 확대 및 컴퓨터 이용의 급격한 증가에 따른 부작용으로 컴퓨터 보안문제가 중요하게 대두되고 있다. 이에 따라 침입자들로부터 침입을 줄이기 위한 침입탐지시스템에 관한 연구가 활발하다. 더욱이 보안을 요구하는 시스템들의 환경이 다양하여 그에 적합한 보안정책을 수립하여 관리하기가 어려워지고 있다. 따라서 침입자들로부터 위험을 줄이기 위해 침입탐지 및 대응을 위한 보안정책기반 모델에 관한 연구가 활발하다. 본 논문은 오늘날의 정보통신응용에서 침입탐지요구사항의 복잡한 문제를 해결하기 위한 침입탐지 메카니즘의 설계 방안을 제시한다. 탐지대상을 특권프로세스가 수행할 때 발생하는 시스템 호출 순서 중 비정상적인 시스템 호출을 탐지하여 이를 분산된 각각의 침입탐지 시스템들이 서로 동적으로 공유하여 침입에 대한 대응력을 향상시키는 침입탐지시스템을 설계하고 프로토타입으로 구현하고자 한다.

키워드 : Security, Intrusion Detection

Ⅰ. 서론

최근의 정보통신기반구조는 컴퓨터시스템의 네트워크를 통하여 다양한 서비스를 제공하고 있다. 특히 인터넷은 개방형 구조로 구성되어 있어 서비스 품질의 보장과 네트워크 관리가 어렵고, 기반구조의 취약성으로 인하여 타인으로부터 해킹 및 정보유출 등의 위협으로부터 노출되어 있다.

불법 및 고의로 네트워크를 통하여 컴퓨터시스템에 접근하여 피해를 야기하는 문제에 대한 침입차단, 인증 그리고 접근제어 등의 다양한 방법이 제공되고 있지만 사실상 역부족인 상태이다. 보안위협에 대한 능동적인 대처 및 침입 이후 동일한 또는 유사한 유형의 사건 발생에 대해 실시간으로 대응할 수 있는 침입탐지시스템에 대한 연구가 활발히 진행되고 있다.

일반적인 침입탐지 시스템은 단순한 접근제어 기능을 넘어서 침입 패턴을 데이터베이스로 구축하고 전문가 시스템을 사용하여 네트워크나 컴퓨터시스템의 사용을 실시간으로 모니터링하고 침입을 탐지하는 보안 시스템이다. 침입 탐지기법은 크게 이상침입탐지기법과 오용탐지기법으로 나눌 수 있다. 오용탐지는 알려진 침입 방법들을 수집하여 지식베이스에 유지하고, 동일한 침입유형을 지식베이스 검색을 통한 비교에 의해 침입을 탐지하는 방법이다.

이상탐지는 정상행위로부터 벗어나는 주목할 만한 특이한 패턴을 침입으로 규정하여 침입을 탐지한다. 일반적으로 오용탐지 방법이 많이 사용되지만 새로운 침입패턴과 변형된 침입 패턴을 탐지할 수 없는 문제가 있어 해결책으로 정상 및 비정상 행위로부터 침입을 탐지하는 이상 침입탐지 연구가 진행되고 있다.

이에, 탐지대상을 특권프로세스가 수행할 때 발생하는 시스템 호출 순서 중 비정상적인 시스템 호출을 탐지하여 이를 분산된 각각의 침입탐지 시스템들이 서로 동적으로 공유하여 침입에 대한 대응력을 향상시키는 침입탐지시스템을 설계하고 프로토타입으로 구현하고자 한다.

Ⅱ. 관련 연구

침입이란 1980년 Anderson에 의해서 침입의도를 가지

고 비인가된 정보로 접근 및 분석, 정보조작, 그리고 시스템의 무기력화에 대한 고의적 시도에 대한 모든 가능성을 탐지하는 것이라고 정의하였다.

Anderson은 서비스 거부원인, 백도어 생성, 바이러스 생성, 공격용 도구에 의한 컴퓨터자원의 무결성, 신용성, 손상을 시키고자하는 시도를 침입으로 정의하였다.

침입은 크게 두 가지로 정의 할 수 있다. 먼저 컴퓨터가 시용하는 자원의 무결성, 비밀성, 신용성을 저해하는 일련의 행위들의 집합을 침입이라 할 수 있고, 다음으로는 컴퓨터시스템의 보안정책을 파괴하는 행위를 침입이라 할 수 있다. 이러한 침입의 행위의 결과에 따라서 이상 침입과 오용침입으로 분류한다.

컴퓨터면역시스템을 기반으로 한 침입탐지시스템은 네트워크를 통하여 동질형의 여러 호스트에 분산된 침입탐지시스템을 포함하고, 각각의 호스트는 자신의 침입시스템을 통하여 호스트에서 발생하는 이벤트들을 모니터링 하면서 이미 설정된 정상 이벤트 패턴정보에 따라 침입 여부를 판단한다. 이 때 각각의 호스트에서 감시하는 대상은 모든 호스트에서 존재하는 동일한 객체이며, 각 호스트는 상기 객체에 대한 비정상이벤트를 공유하면서 새로운 침입으로부터 전체의 시스템에 대한 면역력을 향상시킨다.

면역시스템은 다계층 방어특징, 분산탐지특징, 다양성 특징, 새로운 외래 패턴에 민감하게 대응하는 특징, 불안한 탐지 특징, 병원체 탐지 및 대응하는 특징이 존재한다.

동물의 육체는 피부 및 점액막과 같은 정적인 보호막, hp 및 온도와 같은 생리적 조건, 일반적인 염증 대응, 그리고 B Cell과 T Cell 메커니즘에 의한 적응력, 대응력을 통해 외부로부터 병원체 침입에 대한 다계층으로 방어하는 특징이 있다.

면역시스템에서 정적인 보호막과 탐지자에 의해 적응형 대응에 대하여 도시하였다. 병원체가 보호막을 파괴하고 육체에 침입하면 자연면역시스템은 탐지자의 존재 유무를 반대측 선택방법에 의해 판단 후 만일 면역력을 증가시키고 병원체를 살균세포에 의해 제거한다.

2.1 침입탐지 모델 유형

2.1.1 Dorothy Denning Model

이 모델은 시스템의 비정상적인 형태의 사용에 대하여 시스템의 로그기록을 모니터링 함으로 침입을 탐지하는 모델로 미리 정의된 통계적인 방법들을 사용하여 시스템의 행위를 계산하는 변수들을 이용한다.

2. 1. 2 Shiuh-Pyng Shich Model

직접관계에서 시스템의 상태와 상태 이전, 주체와 객체 사이의 간접관계를 나타내는 규칙으로 정의된다. 시스템 상태는 감시추적에서 캡처되고, 보호그래프로 표현된다.

시스템 상태는 방향에 있는 보호그래프G(V, E, C, F)로 표현되고, 이 그래프는 노드들의 집합 V, 레이블에 있는 간선들의 집합 E, 보호집합들의 집합 C, 합법적인 흐름 행렬 F로 구성된 구조를 가진다.

즉, 노드들의 집합 V는 주체와 객체들로 구성되고 주체 SI와 객체 CI는 그래픽 보호로 표현되고 접속오퍼레이션은 노드 V1과 V2사이에서 발생하고 Present relation으로 표현된다. 알려진 침입 패턴들은 데이터와 권한의 흐름에 대하여 네 가지형태로 특성화시킨 모델이다.

2. 1. 3 Sandeep Kumar Model

Jensen에 의해서 CPN에 근거하고 있으며, 침입행위는 칼라페트리 네트로 표현하고 네트에서 하나 이상의 초기 상태들과 하나의 마지막 상태는 모델에서 매칭을 정의하기 위해서 사용되는 모델이다.

2. 1. 4 DARPA/ITO

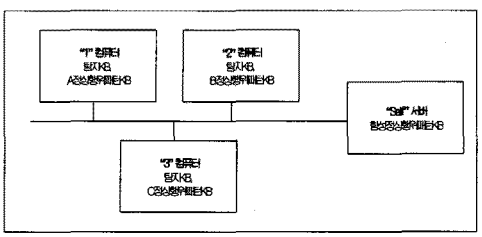
미 국방부의 DARPA(Defense Advanced Research Program Agency), ITO(Information Technology Office)는 부정행위를 탐지하기 위해 1996년부터 1999년까지 30여개의 과제를 프로그램으로 추진하였으며, JAM은 침입패턴에 대한 분산 환경에서 에이젠트기반 데이터 마이닝시스템 모델이다.

III. 본론

보안시스템의 형태인 침입탐지면역시스템은 침입탐지의 오류를 줄이고 침입을 탐지하였을 경우 보다 효과적인 대응을 하는 것이 목적이다.

분산된 각 호스트에 설치된 침입탐지시스템이 서브감시시스템을 통해 특권프로세스에 의해 생성되는 시스템 호출 순서 정보를 추출하여 이미 설정된 비정상 호출 패턴과 정상 시스템 호출 패턴과 서로 비교하여 비 정상시스템을 탐지하고 이를 분산된 침입탐지 시스템들과 서로 동적으로 공유하여 모든 호스트에 설치된 침입탐지시스템들이 새로운 침입에 대한 지식을 증가하여 침입으로부터 면역력을 향상시키는 컴퓨터 면역 시스템을 기반으로 한 침입탐지시스템을 설계 한다.

제안된 시스템에서 침입탐지면역시스템은 이미 알려진 침입에 대한 비정상 행위 시스템 호출 패턴으로 구성된 탐지자 지식베이스와 패턴지식베이스를 포함하고, self 서버는 동질형 시스템으로부터 침입탐지대상 프로세스가 정상적으로 수행하면서 생성한 시스템 호출 패턴을 수집하는 방법으로 구성한 합성정상행위 패턴지식 베이스를 포함한다.



〈그림 1〉 침입탐지 시스템 구조
Figure 1 System configuration of intrusion detection

3.1 정상적인 생성부

정상적인 생성부는 각 컴퓨터가 정상 상태에서 사용자가 정상적인 수행을 할 때 발생하는 프로세스의 시스템 호출 순서를 로컬 Self 수집기를 통하여 수집한 후에 패턴생성기를 통하여 구성한다.

생성기는 입력된 프로세스의 시스템 호출 순서를 크기단위로 분리하여 시스템 호출 패턴을 트리로 표현한다. 프로세스에 의해서 생성되는 시스템 호출에 대한 정상 시스템 호출 패턴트리를 구성한 것은 프로세스가 수행하면서 연속적으로 시스템 호출을 생성하면 생성되는 순서에 따라서 시스템 매핑 테이블에 시스템 호출이름을 등록하고 번호를 부여한다. 계속해서 발생하는 시스템 호출들에 대해서는 시스템호출 매핑 테이블을 통해 등록번호를 변경한 후 시스템 호출 이름 단위로 시간 축으로 시프팅 하면서 시스템 호출 패턴들을 생성한다. 생성한 시스템 호출 패턴들은 자주 발생하는 패턴에 대해 추후 검색을 빠르게 하기 위해서 패턴 발생빈도에 따라 트리를 구성한다.

3.2 탐지 수행부

탐지 수행부는 이미 잘 알려진 침입 패턴 정보를 저장한 탐지자 KB(Knowledge Base)와 관리하는 탐지 갱신자, 정상패턴 생성부로부터 전달되는 특권프로세스의 정상행위 패턴을 저장한 정상 패턴 KB와 이를 관리하는 패턴 갱신자와 감사서브시스템에서 제공하는 감사 레코드를 수집하는 감사레코드수집기와, 수집된 감사레코드로부터 시스템 호출을 분리하여 해당되는 침입지부를 가동시켜 침입을 탐지하는 침입탐지엔진과 침입발생을 알리고 해당 프로세스를 강제로 종료시키는 침입보고 및 대응부로 구성된다.

3.3 비정상적인 행위 탐지부

비정상적인 행위의 경우 패킷의 통계정보를 갖고 침입 판정을 한다. 서비스 공격거부와 같은 비정상적인 행위의 탐지는 특정 호스트로 유입되는 패킷 카운터에 기반하여 탐지하게 된다. 침입탐지면역시스템의 침입사건 목록에 서비스 거부공격과 관련된 목록을 포함하고 있으며 프로토콜의 목록을 갖고 있다. 특히 패킷서비스 거부공격에 의한 침입탐지 방식은 주어진 시간 내에 침입탐지 목록을 정의하고 있는 침입사건 항목에 해당하는 패킷이 임계치 이상 발생하였을 경우에 탐지하는 방식으로 임계치 알고리즘은 (1)과 같으며, Q의 알고리즘은 (2)와 같다.

$$T^2 = a_1 s_1 + a_2 s_2 + \cdots + a_n s_n \quad \cdots\cdots (1)$$

T^2 : 비정상적인 행위를 추출하는 기준

$a_1 a_2, \cdots a_n$: 임계설정계수

$S_1 S_2 \cdots S_n$: 측정부분의 통계 값

$$Q = \sum_{k=1} D_k \times 2^{-rtk} \quad \cdots\cdots (2)$$

Q : 현재까지의 발생 총계

k : 발생사건의 인덱스

DK : k번째 감사자료와 (k+1)번째 발생사건의 데이터변화량

t_k : 가장 최근에 발생한 데이터와 k번째 데이터간의 시간차

r : Q값의 감소율

침입탐지면역시스템은 침입사건 목록을 정의하고 있는 항목과 일치하는 패킷에 대한 지속적인 감시가 필요하며 연속적인 패킷 수신에 설정되어 있는 시간 내에 발생하였는가를 판단할 수 있는 구조가 필요하며, 침입사건목록으로부터 패킷의 프로토콜과 목적지 포트번호에 기초하여 해당 패킷의 조건에 일치하면 침입이 탐지되도록 설정되어 있고 침입사건 목록과 패킷의 목적지 주소에 기초하여 해당 호스트의 정보를 테이블에 추가하게 되는데 테이블에 호스트정보가 존재하지 않는다면 해당 패킷에 적당한 호스트정보를 생성하여 생성된 호스트의 카운터를 기초화하고 시작 시간을 설정한다. 일치하는 호스트 정보가 테이블에서 검색되면 해당 호스트 목록의 카운터를 검색 한다. 검색결과 카운터가 0이라면 시작 시간을 기록하고 카운터를 증가시킨다. 증가된 카운터가 침입사건의 임계치와 동일한가를 검사하고 만약 호스트 목록의 카운터와 침입사건 목록의 카운터와 침입사건목록의 임계치와 동일하면 카운터를 초기화하고 침입사건 판정을 계산한다. 계산된 시간 간격이 침입사건의 시간 간격보다 작다면 침입이 발생한 것으로 판단한다.

IV. 성능평가

제안한 모델의 타당성을 입증하기 위하여 모델에 대한 프로토타입을 단일 시스템에서 구현하였다. 제안 한 모델의 프로토타입은 탐지대상 프로그램들에 대한 각각의 탐지자 KB를 구성한 후, 탐지를 수행 하던 중 프로그램을 수행시키는 프로세스의 행위가 비정상적인 경우, 이를 침입이라 판정하고 침입에 사용된 수신지주소, 서비스종류, 포트번호, 그리고 탐지 시간에 관한 정보를 출력 후, 현재 침입에 사용된 프로세스를 강제로 종료시켜 침입에 대응하도록 하였다.

4.1 프로타입 구현

성능평가에 사용된 프로토타입은 패턴길이를 가변시켜 패턴길이에 따라 탐지시간의 의존도를 식별하고, 표준모델을 반복하여 무한정으로 시스템 호출을 발생시켜 여러 개의 프로그램들을 동시에 수행시켜 이를 통해 컴퓨터의 성능에 따라 침입탐지면역시스템의 탐지 능력을 평가하였다. 프로그램을 무한정 가동하여 제안한 모델에서 탐지 대상 프로그램이 무한정 발생할 때 제안한 알고리즘의 처리 부하에 따른 탐지 능력을 평가한다.

4.2 다중공격과 IP 스푸닝 탐지

침입탐지면역시스템은 호스트에 다중으로 침입을 시도하는 공격에 대하여 쉽게 탐지 할 수 있고, 침입을 탐지하기 어려운 단일모델에 대하여 효과적으로 탐지할 수 있도록 하였다. 먼저 RST패킷을 보내 연결을 강제로 종료시키거나 호스트를 다운시키는 SYN 플러딩 공격 같은 침입 이벤트가 발생될 때는 각

침입탐지시스템의 캐쉬로 보내어 이를 참조하여 동일 수신 주소와 포트번호를 같은 패킷의 경우 침입판정을 내리게 된다.

스프핑 공격시 공격에 대한 RST패킷을 보내어 강제로 접속을 단절시키고 상대방 호스트와 연결을 가로채어 정보를 침입탐지면역시스템으로 전달하게 된다. 이 정보를 전달 받은 침입탐지면역시스템은 수신지 주소와 서비스종류, 포트번호와 비교하여 공격을 탐지하게 된다. 기존의 단일 모델에서는 판단하기 어렵고 정보의 상호교환이 이루어지는 침입탐지면역시스템에서는 탐지가 가능하도록 하였다.

〔표 1〕 IP Spoofing 탐지 결과
Table 1 detection of IP Spoofing

Host Attack
Alsrt ID : TCP-RST
Time : 2008. 11. 11. 11:30:09
Source Address : 129.254.245.109
Destination Address : 129.254.245.107
Source Port : 22230
Destination Port : 18

Attack for SYN Flooding
Alsrt ID : SYN-Flood
Time : 2008. 11. 13. 14:30:09
Source Address : 129.254.245.109
Destination Address : 129.254.245.107
Source Port : 22236
Destination Port : 56

Alsrt ID : TCP-RST
Time : 2008. 11. 11. 11:30:09
Source Address : 129.254.245.109
Destination Address : 129.254.245.107
Source Port : 22230
Alsrt ID : SYN-Flood
Time : 2008. 11. 13. 14:30:09
Source Address : 129.254.245.109
Destination Address : 129.254.245.107
Source Port : 22236

4.3 탐지 및 추적

침입탐지면역시스템의 성능에 있어 전체적인 탐지시간은 시스템 환경과 운영체제의 메모리 관리방법 등 여러 가지 요인에 의해 공격 시도 횟수에 따라 다르지만 신뢰성을 갖기는 힘드나, 자주 사용하는 탐지프로그램을 탐지할 경우와 패턴 길이가 길고 동시 수행프로그램 수가 많을 경우 제안한 모델이 탐지시간 측면에서 빠름을 알 수 있고, 또한 중요한 요소인 탐지 정확도를 측정하기 위하여 호스트 주소와 호스트 서비스프로토콜, 포트 등에 등록하여 탐지시 사용하도록 하여 평가한 결과 탐지 시간이 짧아짐을 알 수 있다.

또한 경로추적을 위해서는 프로토타입에서 수집된 정보들을 시간 값과 탐지된 영역이 면역시스템으로 추정하고 동작을 분석하기 위해 호스트로 Ping을 발생시켜 정보를 전달하게 한다. 전달된 패킷의 수신주소와 프로토콜정보, 패턴매칭을 하여 일치하는 패킷정보를 시간값과 함께 침입탐지면역시스템으로 전달하게 되며 호출 순으로 경로를 예측하게 된다.

V. 결론

본 논문에서는 침입탐지시스템을 바탕으로 새로운 침입탐지면역시스템모델을 제안하고 이를 설계 및 프로토타입을 구현하고 그 타당성을 확인하였다.

제안한 침입탐지 면역시스템모델은 어떤 공격이 프로세스 행위를 정상행위와 다르게 하는 경우 이를 침입으로 탐지할 수 있는 비정상행위 탐지방법을 기반으로 하는 침입탐지 시스템이다. 특히, 제안한 모델에서 침입탐지 면역시스템모델들은 컴퓨터에서 분산되고 분산된 침입탐지면역모델들 중 어느 하나가 프로세스에 의해 발생된 시스템 호출 순서 중 비정상적인 시스템 호출을 탐지한 경우 이를 다른 침입탐지 프로세스 모델과 서로 동적으로 공유한다.

제안한 모델의 타당성을 입증하기 위해 모델에 대한 프로토타입에서 실험하였으며, 실험결과 단일시스템에서 탐지하기 어려운 다중공격 IP스푸핑 등의 탐지에 효과적임을 알 수 있었다.

따라서 제안한 침입탐지 프로세스 모델은 공격을 받으면 받을수록 전체 침입탐지면역시스템모델의 면역력이 향상되므로 새로운 침입을 효과적으로 방지할 수 있다. 이와 같은 접근제어는 최근에 연구가 활발하게 진행되고 인공생명의 새로운 적용 연구 분야를 제시하고 있다.

향후 연구과제는 프로세스의 모든 정상행위에 대한 시스템 호출 패턴들을 관리하는 서버의 효율적인 구축과 현재 구현된 프로토타입을 전체 분산시스템으로 확장 구현하여 많은 사용자들이 사용하는 프로그램들을 대상으로 적용하고, 이기종간의 감사 데이터 표준화를 통해 제안한 모델을 이기종 환경에서 확장 시키는 연구가 필요하다.

참 고 문 헌

〔1〕 한국컴퓨터학회,"보안정책기반침입탐지시스템 모델 설계", 2003. 12.

〔2〕 Dan Wlash, "Elevating Security Brst Practices: SELinux", November, 2003.

〔3〕 R. Sahita, S. Hahn, K. Chan, K. McCloghrie, "Framework Policy Information Base," RFC 3318, IETF Network Working Group, March, 2003.

〔4〕 J. Strassner, B. Moore, E. Ellesson, "Policy Core weight Directory Access rotocol(LDPA) Schema, "RFC 3073, IETF, Feb 2003.

〔5〕 J.Bournelle, G. Valadon, D. Binet, S. Zrelli and J. Combes, "AAA Considerations within Several NEMO deployment Scenarios", 1st workshop on network mobility, japan, jan. 2006.

〔7〕 Yongro Park, A Statistical Process Control Approach for network intrusion detection, Ph. D Georgia Institute of Technology, 2005.

〔8〕 Shyam Varan Nath, Intrusion detection in wireless networks: A data mining approach, MS Florida Atlantic University, 2005.