2004년도 대한전기학회 하계학술대회 논문집 2004.7.14-16

호스트 상태 변화 관찰을 통한 침입 탐지

곽미라, 조동섭
이화여자대학교 과학기술대학원 컴퓨터학과

Intrusion Detection Based on Host Status Transition Monitoring

Mira Kwak, Dong-sub Cho
Dept. of Computer Science and Engineering, EIST, Ewha Womans University

Abstract - 현재 주로 사용되는 네트웍 침입 탐지 기법은, 사람의 이해를 바탕으로 분석되고 저장된 침입 시그너쳐를 기반으로 침입을 판별하는 것이다. 이러한 방법은 아직 알려지지 않은 침입에 대해 무력하다는 한계를 가진다. 이에 본 연구에서는 사람의 분석과 지식에 의존하지 않는 방법을 제안하여 그러한 한계를 극복하고자 하였다. 침입은 호스트의 컴퓨팅과 네트워킹 자원을 사용할 수 없게 되는 것이라고 볼 때, 네트웍 트래픽과 관련하여 호스트의 자원 사용 상태가 앞으로 어떻게 진행할 지 알 수 있다면, 해당 침입에 대한 사전지식 없이도 위험에 대비할 수 있다. 본 논문에서는 자원의 가용성 측면에서 호스트 상태를 설명하는 모델을 설계하고, 이 모델이 네트웍 트래픽 진행에 따른 호스트 상태 변화 추이의 예측하고 침입을 탐지하도록 하였다.

1. 서 론

컴퓨터와 네트웍의 사용이 일반화되면서 그에 대한 침입의 위협도 증가했다. 이에 따라 컴퓨터 및 네트웍 침입에 대처하는 데 대한 연구가 활발히 진행되고 있다. 이러한 분야의 연구 주제들 중 침입 탐지 연구는 '컴퓨터와 네트웍 자원을 대상으로 악의를 가지고 행하여진 행동들을 식별하고 그에 대응하는 방법과 절차'에 관한 것이다. 현재까지 연구된 침입 탐지 기법은 크게 두 가지로 나뉘는데, 오용탐지와 비정상탐지가 그것이다. 오용탐지는 사람에 의해 분석되어 룰로서 저장된 침입 시그너쳐에 기반하여 침입을 찾아내는 것이다. 현재 실용화되어 널리 쓰이는 침입 탐지 기법들 중 많은 것이 이에 해당되는데, 이는 알려진 침입을 정확하게 탐지할 수 있으나 알려지지 않은 침입에 무력한 한계를 가진다. 다른 대표적인 접근 방식인 비정상탐지는 사용자나 시스템의 정상적인 행동 정보를 바탕으로 이로부터 벗어난 행동을 침입으로 간주하는 기법이다. 이 방법은 모르는 침입에 대응하지 못하는, 룩 기반 기법의 단점을 해결하지만, 침입이 아닌 경우를 침입으로 간주하기 쉬운 약점을 가진다. 이에, 결과의 높은 정확성을 유지하면서 알려지지 않은 침입에도 대응하는 기법의 개발이 필요하다.

오용탐지 및 비정상탐지 기법은 모두 사람의 판단과 작업에 의존한다. 오용탐지기법의 경우, 침입 식별의 기준이 되는 규칙은 사람의 이해를 바탕으로 생성되므로, 그 결과는 명백히 사람의 판단과 작업에 의존적이다. 비정상탐지의 경우, 그 학습내용에 대해 이미 내려진 정상 여부의 판단이 사람의 이해를 바탕으로 하므로 역시 사람의 생각에 의존적이다. 사람의 판단에 의존한 지식은 감추어진 실마리를 간과할 수 있다. 본 연구에서는, 사람의 판단을 배제함으로써, 이렇게 과거 데이터 분석 과정에서 간과될 수 있는 실마리를 찾아내어, 새로운 양상을 보이는 현상 파악에 유용하게 사용하고자 한다. 즉, 사람의 개입을 최소화하고 대상 시스템의 상태 변화 자체에 최대한 초점을 맞추어 새로운 침입에도 대응할 수 있는 탐지 기법을 제안하고자 한다.

2. 침입 탐지 기법

침입 탐지 기법의 대표적인 두 방법 중 하나는, 공격에 관한 축적된 지식을 사용하여 특정 공격이 일어나고 있음을 발견하는 오용탐지 기법이다. 또 다른 하나는 감시 대상이 되는 시스템의 정상 행위에 관한 참조 모델을 생성하고 이에서 벗어나는 경우를 발견하여 침입으로 여기는 비정상행위탐지 기법이다. 두 기법이 매우 달라 보이지만, 여기에는 모두 시스템이나 사용자의 현재까지의 행위나 그에 일어난 사건에 관한 인간의 이해가 바탕이 된다는 공통점이 있다. 과거 데이터 분석을 바탕으로 하는 기법은, 새로운 양상을 포함하는 미래 데이터에 대해 잘못된 분석을 도출할 수 있다. 이에 본 연구에서는 과거 데이터를 인간의 이해에 근거하여 분석하는 대신, 감시 대상이 되는 시스템의 상태 자체에 초점을 맞추는 방법을 제안하고자 한다. 즉, 지금 대상 호스트 시스템에 일어나고 있는 일들이 그 시스템의 상태를 위험하게 할 것인지 판단하여, 위험의 가능성이 있는 경우, 위험을 야기하는 일련의 행위를 침입으로 판정하는 기법을 설계하고자 한다. 제안하는 기법을 설계하기 위한 하위 기법을 설계하기 위해, 기존에 사용된 기법들을 응용한다. 이러한 기법들에는 다음과 같은 것들이 있다.:

오용탐지 기법의 구체적인 접근 방법에는 전문가 시스템, 시그너쳐 분석, 페트리넷, 상태전이분석 등의 기법이 있다. 전문가 시스템 기법은 공격에 관한 규칙집합을, 시그너쳐 분석 기법은 탐색이 용이한 데이터 패턴 형태의 공격 시나리오들을, 상태전이분석 기법은 상태전이 다이어그램 형태로 저장된 공격 정보를 유지한다. 비정상행위탐지 기법을 위해서는 통계적 기법들이 사용되어 시간에 따라 샘플링된 시스템 행동 관련 변수들의 평균 및 표준편차와 같은 통계적 값이 기준이 되어 침입이 판정된다. 이 밖에, 정상행위에 관한 규칙집합을 유지하는 전문가 시스템 기법, 사용자의 고수준 작업을 관찰하여 사용자 정상행위를 모델링하고 비정상행위 탐지의 기준으로 삼는 기법, 정상 행위와 비정상 행위에 관한 테이블을 유지하며 그로부터 감사데이터를 검색하는 면역학적 기법 등이 비정상행위탐지 방식의 침입 탐지 기법에 사용된다.

제안하는 침입 탐지 기법을 위해 오용탐지 및 비정상행위탐지에 사용된 기본적 접근 기법들을 사용하되, 인간의 의식에 의한 시스템 행동의 오해를 방지하고자 다른 방식으로 적용한다. 3장에서 이를 설명한다.

3. 호스트 상태 변화 기반 침입 탐지

3.1 네트웍 트래픽과 호스트 상태 변화

침입은 그것이 목적하는 내용과 행해지는 대상에 따라 여러 가지로 나뉜다. 본 논문에서 제안하는 침입탐지 시스템은 네트웍을 통해 이루어지는 침입만을 탐지 대상으로 하였다. 서비스 거부 공격 류의 공격, 실질적 공격 전 정보 수집을 위한 탐색 행위 등이 이에 해당한다.

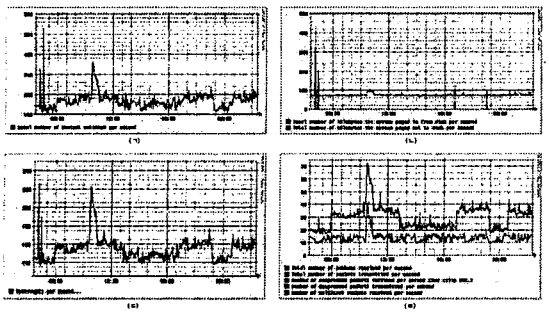

그림 1 (가)인터럽트 (나)문맥교환 (다)페이징 (라)네트웍 트래픽

그림 1은 자원 소비 측면에서 호스트 상태를 설명하는 값들과 네트웍 트래픽 관련 값들을 측정한 예로서, 이 값들 사이의 명시적 관련성을 보인다. 이를 바탕으로 본 연구는 네트웍 사건들과 호스트 상태 변화 사이에 밀접한 관련이 있음을 가정한다.

3.2 호스트 상태 변화 기반 침입 탐지 개요

본 연구에서 목적으로 하는 침입 탐지 시스템은 그림 2와 같이 구성된다. 호스트의 상태를 관찰하는 모듈과 네트웍 트래픽을 관찰하는 모듈이 관찰 내용을 끊임없이 기록한다. 수집된 내용은 네트웍 트래픽 모델 생성 모듈과 호스트 상태 모델 생성기에 의해 처리되어 네트웍 사건들과 호스트 상태 변화 사이의 관계를 발견하는데 사용된다. 발견된 네트웍 사건과 호스트 상태 변화 사이 관계 정보는 호스트 상태 관찰 모듈과 네트웍 트래픽 관찰 모듈의 실시간 정보와 함께 예측 모듈에 입력되어 호스트의 미래 상태를 예측하는데 사용된다. 침입 판정 모듈은 예측된 호스트 상태에 위험의 가능성이 있는 경우 침입 경보를 발생한다.

그림 2에 나타난 목적 시스템의 개요 중 본 연구의 핵심이 되는 호스트 상태 변화 예측 부분의 동작은 그림 3과 같이 설명된다. 네트웍 트래픽 관찰 모듈은 트래픽의 흐름에 적응적인 크기의 윈도를 사용하여 현재 네트웍 트래픽에서 발견되는 기본 행동들을 발견한다. 발견된 네트웍 행동들은 네트웍 트래픽 관찰 버퍼에 저장된다. 저장된 내용으로부터 의미있는 네트웍 사건이 예상되면, 해당 네트웍 사건이 호스트 상태에 야기하는 변화를 현 호스트 시스템의 상태에 적용하여 호스트 시스템의 상태 변화를 예측한다. 예측은 호스트의 상태를 설명하는 변수 값의 추정을 통해 이루어지는데, 그 결과가 미리 정의된 호스트 상태의 안전도 평가 기준에 비추어 어떠한 안전도를 의미하는지에 따라 적절한 보안 경고가 발생된다.

4. 호스트 상태 변화 모델 설계

4.1 호스트 상태

호스트의 상태를 자원 소모의 측면에서 설명하기 위해 관련 내용을 다음과 같이 관찰하였다.:

- 프로세스 생성률
- 문맥교환 발생률
- CPU 사용률
- 인터럽트 발생률
- 메모리 사용통계: 스왑 페이지, 페이지 량, 해제 현황, 버퍼로 사용된 페이지 량, 캐쉬된 비율
- 디스크 입출력 통계: 쓰기/읽기 발생률, 입출력 통계
- 네트웍 통계: 송수신 패킷 수/크기, 드롭된 패킷 수/크기, 오류 발생 수, 사용 소켓 수
- 커널 테이블: 미사용 캐쉬 엔트리, 파일 핸들러, inode 핸들러, 수퍼 블록 핸들러 등
- 실행 큐: 실행 큐 길이, 프로세스 목록 내 프로세스 수

관찰 내용의 항목이 많고 항목 사이 연관성이 커, 서로 독립적인 적은 수의 항목으로 줄이고자 ICA 알고리즘을 적용하였다.

4.2 호스트 상태 변화 모델

호스트 시스템에 관한 모델을 유지하는 아이디어는 기존의 침입탐지 기법들에서도 발견된다. 저수준이나 고수준에서 호스트 시스템의 정상 행동들을 프로파일로 만들

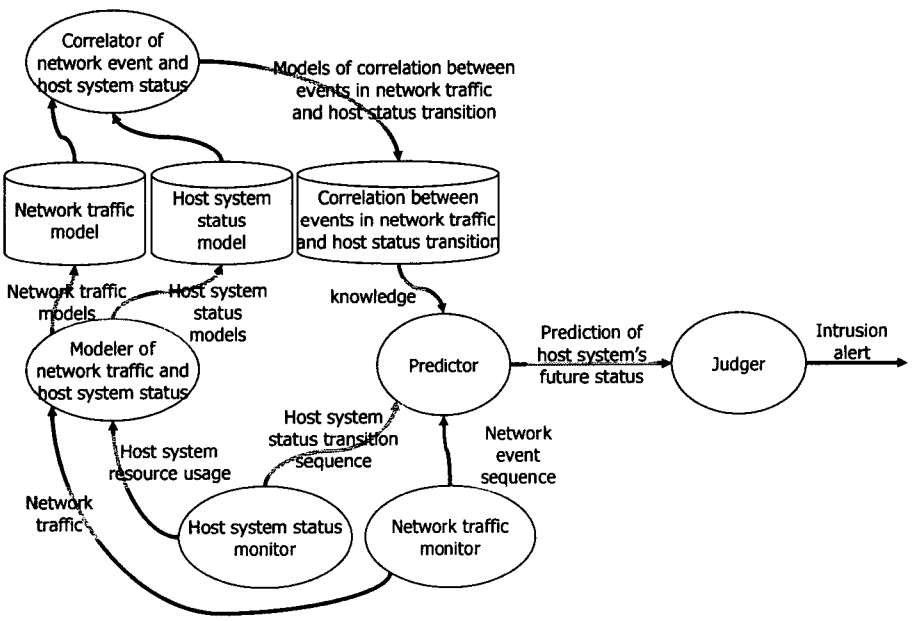

그림 2 침입 탐지 시스템의 전체적 흐름

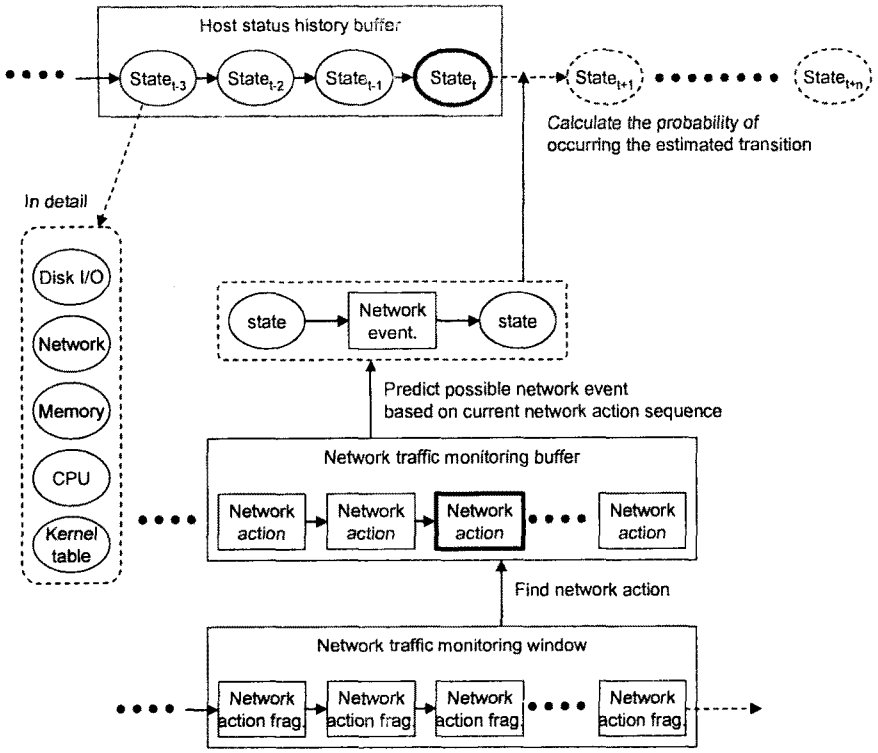

그림 3 호스트 상태 예측

고 정상 영역을 정의하는 임계값을 정하여 비정상 행위 탐지의 기준으로 삼는 것이 전형적인 기법이다. 그러나, 본 연구에서는 다른 관점에서 다른 방식으로 호스트 시스템에 관한 모델을 만들고 사용한다. 본 연구에서는 사람의 해석을 가능한 한 배제하고 시스템 상태 자체에 초점을 맞추고자 하였다. 따라서 호스트 시스템의 상태에 대한 정상 여부 판단은 기초 데이터에 포함될 수 없고, 호스트 모델은 정상 행동 모델이 아닌 다른 종류의 것이어야 한다. 또한 호스트에 관한 모델은 그 호스트의 상태 예측에 사용될 수 있는 것이어야 하며, 앞서 구한 상태 설명 변수로써 표현 가능한 것이어야 한다. 이에, 본 논문에서는 상태 설명 변수 값의 변화량으로 표현되는 호스트 상태 전이를 관찰 심볼로 사용하여 HMM을 이용한 모델 설계를 수행하였다.

호스트 상태 변화 모델링은 실시간 호스트 상태 관찰 모듈이 읽어 처리한 값들의 시퀀스를 기반으로 HMM의 매개변수를 결정하는 과정이다. HMM의 매개변수 결정은 주어진 관찰열이 해당 모델로부터 나왔을 확률이 최대가 되도록 모델을 조정하는 과정을 반복하여 이루어진다.

5. 호스트 상태 변화 예측과 침입 판정

실시간 네트웍 트래픽 관찰 모듈은 추출된 네트웍 사건의 예상 시퀀스를 바탕으로 호스트 상태에 일어날 일련의 변화 시퀀스를 생성한다. 해당 변화 시퀀스를 통해 궁극적으로 호스트가 위험에 처할 것으로 판단되는 경우, HMM에 해당 시퀀스를 입력하여 그러한 일이 일어날 확률을 계산한다. 그 결과가 충분히 높으면 침입이 일어났을 가능성이 있는 것으로 간주한다.

6. 결 론

본 논문에서는 감시 대상이 되는 호스트의 상태 변화를 기반으로 침입을 탐지하는 시스템의 기본을 고안하였다. ICA를 사용하여 호스트 상태를 설명하는 축약된 변수들을 추출하였고, 호스트 상태 변화를 설명하고 예측하기 위해 HMM을 사용하였다. 또한, 네트웍 트래픽으로부터 의미있는 사건들의 시퀀스를 추출하여 호스트 상태 변화를 일으키는 원인으로 삼았다. 앞으로, 고안한 침입 탐지 기법의 부분적인 요소 아이들의 정확성을 검토하고 검토 결과를 바탕으로 이를 개선하고자 한다.

이 논문은 2004년도 두뇌한국21사업에 의하여 지원되었음.

[참 고 문 헌]

[1] Ghosh, A.K., Michael, Ch., Schatz, M., "A Real-Time Intrusion Detection System Based on Learning Program Behavior", Recent Advances in Intrusion Detection, Lecture Notes in Computer Science, Vol.1907, pp.93-109, 2000

[2] Corodetski, V. Kotenko, I., "Attacks against Computer Network", Recent Advances in Intrusion Detection, Lecture Notes in Computer Science, Vol.2316, pp.219-238, 2002

[3] Cockcroft, A. "Sun Performance and Tuning: Sparc & Colaris", 1994.

[4] 최종호, 조성배, "침입탐지 시스템을 위한 은닉 마르코프 모델의 적용", 정보과학회논문지:소프트웨어및응용, 6호, 제28권, pp.429-438, 2001