2002년 한국정보처리학회 춘계학술발표논문집 제9권 제1호

다중 척도 결합 기반 침입탐지 시스템

박혁장, 조성배
연세대학교 컴퓨터과학과
e-mail : twinkler@candy.yonsei.ac.kr

Intrusion Detection System based on Multiple Measure Bonds

Hyuk-Jang Park, Sung-Bae Cho
Dept. of Computer Science, Yonsei University

요 약

본 논문의 침입탐지시스템에서는 퍼지 추론을 통한 대표적인 세가지 다중 척도 결합을 제안하였다. 그 중 시스템 호출 척도에서는 권한이동 정보만을 이용한 감사자료 축약방법으로 기존 HMM 모델의 문제점인 모델링 시간 단축을 가능하게 하였고, 프로세스 척도에서는 권한이동 기반 모듈의 단점을 보완하기 위하여 모든 감사자료에 대하여 통계적 분석방법을 사용을 사용하였다. 파일 입출력 척도에서는 상태전이 모니터링을 통하여 파일에 대한 접속 상태 변이를 분석하는 방법을 제안하였다.

1. 서론

침입탐지 시스템이란 내부자의 불법적인 사용, 오용 또는 외부 침입자에 의한 중요 정보 유출 및 변경을 알아내는 것으로서 각 운영체제에서 사용자가 발생시킨 키워드, 시스템 호출, 시스템 로그, 사용시간, 네트워크 패킷 등의 분석을 통하여 침입여부를 결정한다[1]. 요즘 사용되고 있는 서버 컴퓨터 시스템은 C2 이상의 보안 감사 프로그램을 자체적으로 지원하여 모든 이벤트를 기록하기 때문에 쉽게 정보를 얻을 수 있다. 침입탐지 기술의 세계적인 현황은 아직 기술적 미성숙 상태이지만 역동적으로 다양한 실험적 제품이 개발되고 있다. 국내의 경우 연구수준의 침입탐지시스템에서는 사용자의 정상행위를 모델링 하기 위하여 신경망과 은닉 마르코프 모델(HMM) 등 다양한 기술을 시도하고 있다. 하지만 대부분의 상업용 시스템에서는 오용탐지 기법 중 하나인 규칙 기반의 침입탐지 시스템을 개발하고 있기 때문에 새로운 침입에는 취약하고 비정상행위 탐지 기법을 적용한 침입탐지 시스템의 경우라도 개별적인 사용자의 행위에 기반을 둔 탐지기술보다는 일반적인 사용 시간 네트워크 접속 수 등이 비정상행위 탐지를 위한 척도로 사용되기 때문에 적절하다 할 수 없겠다. 따라서 본 연구에서는 각 척도(Measure)별 장점에 맞는 모델링 방법을 통하여 최적의 탐지를 얻을 수 있는 통합 침입탐지 시스템을 제안 하였다.

2. 관련연구

본 침입탐지시스템에서는 은닉 마르코프 모델을 이용하여 BSM 데이터에서 발생하는 이벤트들을 모델링하는데 사용하였고 특히 정상행위 모델링을 시스템 호출관련 척도에 적용할 경우 좋은 결과를 얻을 수 있었다[2]. 미국의 아리조나 주립대학이나 뉴 멕시코 대학의 RAID 등에서 제안한 은닉 마르코프 모델 기반 침입탐지시스템은 타 침입탐지기법들에 비해 false-positive 를 최소화 할 수 있으면서 탐지율을 높일 수 있다는 장점으로 인해 많은 관심을 받았다. 하지만 높은 성능에 비해 정상행위 모델링과 침입 판정 시 매우 많은 시간을 소요하는 단점으로 실시간 침입탐지에 적절치 못하다는 지적이 있었다[3]. 따라서 은닉 마르코프 모델을 사용해 실시간 침입탐지를 하기 위해서는 시스템 성능이 비약적으로 개선되거나, 정상행위 모델링이나 침입탐지를 위한 데이터의 획기적인 축약 기법이 필요하다.

2.1 권한이동 감사자료 수집

감사자료의 수집과 축약은 침입 탐지의 첫 단계로서, 최종목표는 아니지만 중요한 위치를 차지하고 있다. 일반적인 축약방법은 수집된 감사 자료 중 탐지에 필요한 자료만을 추출하여 재정렬하는 방법으로 다음 작업을 통하여도 많은 데이터 축약을 할 수 있다. 하지만 하루에도 수백 메가바이트 이상이 발생되는 대

형 서버에서 HMM 모델을 쓰기 위해서는 보다 효과적인 모델링 방법이 제안 되어져야 한다. 본 논문에서는 이러한 문제를 해결하기 위해 권한이동 추출 방법을 선택하였다. CERTCC 2001 년 상반기 해킹 보고에 의하면 최근 호스트 기반 침입탐지 기법에서 버퍼오버플로우 취약성을 이용한 방법과 사용자 권한 설정 오류를 이용한 방법이 거의 90%이상을 차지 하고 있음을 알 수 있었다[4]. 이러한 호스트 관련 침입의 대부분은 시스템의 버그나 사용자의 잘못된 사용을 통해 루트의 권한을 획득함으로써 발생하게 된다. 따라서 정상적인 루트 권한 획득에 관련된 정보를 모델링하면 불법적인 권한 이동을 감시할 수 있으며, 그 결과 대부분의 호스트 기반 침입을 탐지할 수 있다. 게다가 침입탐지의 감시 대상을 효과적으로 줄여 침입탐지를 위한 시스템 자원의 사용을 획기적으로 줄일 수 있기에 실용화 가능성을 보일 수 있다.

2.2 다양한 척도 추출

권한이동 정보를 통한 감사자료 축약은 기존 HMM 모델의 문제점인 모델링 시간 단축을 가능하게 하였지만 관리자로의 권한이동이 아닌 서비스 거부 공격(DOS) 등은 탐지가 불가능하다는 약점을 지니고 있다. 또한 HMM 특성상 비정상적인 행위를 발견하였더라도 공격의 유형과 특징을 파악하기가 쉽지 않다. 따라서 이를 보완하기 위한 다양한 척도들의 분석이 필요하다. 침입탐지에 사용되는 많은 척도들이 과거 연구를 통해 제안되어 왔는데 대표적으로 운영체제에서 발생하는 시스템 호출에 관한 척도와, 프로세스 관련 척도, 파일 입출력에 관련 척도를 들 수 있다. 이러한 각각의 척도들은 침입 유형에 따라 서로 다른 탐지 결과를 보여주고 있다[5]. 시스템 호출의 경우 대부분의 침입유형에 매우 유용함을 알 수 있으며, 파일 입출력의 경우 관리자의 잘못된 설정에 의한 취약성 등을 탐지 하는데 매우 유용함을 알 수 있다. DOS 공격 기법의 경우 프로세스 관련 척도를 통하여 탐지할 경우 좋은 탐지율을 얻을 수 있는데 특성 상 통계적인 방법들이 많이 제안되었다. 또한 HMM 모델을 사용할 경우 비정상행위로 탐지된 침입의 정보를 제공하지 못하기 때문에 이러한 문제에 대한 보안이 필요하다. 이를 위해서 탐지된 모든 척도의 정보를 바탕으로 기존 정의 해둔 비정상행위 패턴과 비교하여 침입 유형을 구분 할 수 있다.

따라서 표 1 과 같은 방법으로 다양한 척도들을 침입 유형에 맞게 적절히 조합한다면 보다 좋은 탐지율을 얻을 수 있을거라 사료된다.

표 1. 척도 별 모델링 방법

척도	모델링 방법
시스템 호출	권한이동 축약을 통한 은닉마르코프 모델
프로세스	각 CPU, I/O 량 에 대한 통계적 분석 방법. Red, Yellow, Green 3 가지 패턴으로 구분
파일 입출력	Subject 와 Object 기반 상태전이 모니터링

3. 침입탐지 시스템

본 논문에서는 다중 척도 분석을 통하여 각 척도에서 적용 가능한 최적의 모델링 방법을 제안하고 모델링 별 취약성 분석을 통하여 발생 가능한 문제점을 다른 척도에서 보완할 수 있도록 하였다.

각 척도의 취약성을 보완하기 위해 3 가지의 모듈을 두어 평가를 하였으며 탐지 모듈의 결과에 따라 적절한 규칙을 두어 나온 다중 평가값을 퍼지 추론화하여 침입유무를 결정하게 된다. 시스템 구조는 다음과 같다 (그림 1).

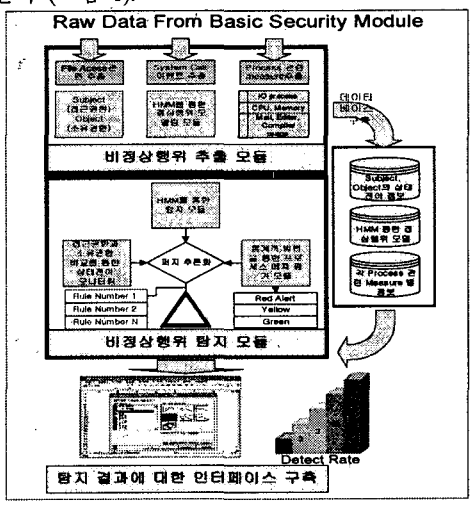

그림 1. 침입탐지 시스템 구조

3.1 권한이동 탐지 모듈

정상적인 권한 이동은 관리자가 일반사용자의 권한으로 들어와 작업도중 SU 명령 등을 통하여 루트의 권한을 획득하거나 일반 사용자가 잠시 슈퍼유저 소유의 시스템 파일(SETUID)로 되어 있는 명령어를 실행시킬 때 발생한다. 이때 SETUID 라는 것은 임시적으로 사용자의 권한을 바꿔줄 수 있는 룰을 파일에 적용시켜주는 것으로써 어떤 사람이든 SETUID 로 설정된 파일을 실행하면 그 파일의 소유 계정으로 프로그램이 실행된다. 일반적인 호스트 침입은 위와 같은 시스템 구조의 취약성을 이용한다. 그림 2 는 버퍼 오버플로우 공격 시 권한이동의 예인데, 일반상태(Q0)에서 fdformat 명령을 사용하면 사용자는 잠시 슈퍼유저의 권한으로 작업을 수행하고(Q1) 해당 작업이 종료된 후 본래의 상태(Q0)로 돌아가야 한다. 그런데 fdformat 작업 도중 버퍼 오버플로우 공격이 발생되면 fdformat 의 작업이 수행된 후 본래의 상태(Q0)로 돌아가지 않고 슈퍼유저의 권한이 그대로 유지되는 상태(Q2)로 전환된다. 결국 해커는 Q2 에서 슈퍼유저의 권한으로 시스템에 접근하게 된다. 그런데 보안모듈이 fdformat 과 관련된 정상적인 권한 이동의 시퀀스를 알고 있다면, 버퍼 오버플로우에 의해 비정상적인 상태(Q2)가 되는 것을 발견할 수 있다. 사용자 권한이동 학습 모델은 이와 같은 정상적인 권한이 이동

되는 시점 전의 정상 시스템 호출 시퀀스를 수집하고 모델링 하여 정상 모델을 생성한 후, 사용자들의 권한이동상태를 비교하여 침입을 탐지한다.

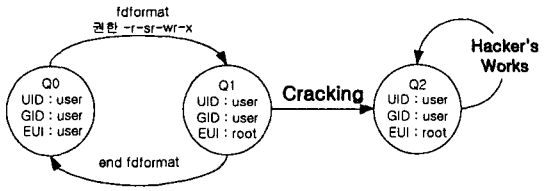

그림 2 버퍼오버플로우 공격 시 권한이동 예

이렇듯 SETUID 나 Symblic Link 등을 통하여 잠시 바뀌는 권한 이동전의 행동들은 정상행위와 비정상 행위를 구분하는 중요한 시점이 된다.

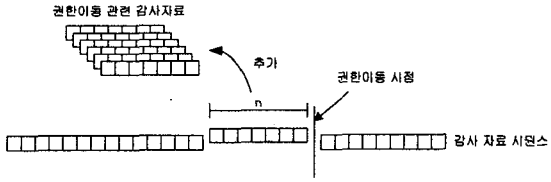

그림 3 권한이동 관련 감사자료 추출 방식

제안하는 모델은 기본보안모듈 감사자료에서 EUID 와 UID 가 변경되었을 경우 그 시점을 기준으로 이전에 사용되었던 일정양의 데이터 시퀀스를 가지고 평가를 하게 된다(그림 3). 이때 기록의 범위는 임의적으로 변경하여 최적의 값을 찾게 된다. 이러한 방법을 통해 EUID 와 UID 가 변경되었을 경우 그 시점을 기준으로 전에 사용되었던 일정양의 데이터 시퀀스를 따로 저장 후 각각 은닉 마르코프 모델에 적용시키게 된다.

3.2 프로세스 척도에 대한 통계적 분석 모듈

프로세스 관련 척도는 권한이동 탐지 모듈에서 탐지하기 어려운 서비스 거부와 그 밖에 방법을 탐지하기 위한 보완책으로 사용될 수 있는데 대표적으로 CPU 사용량, I/O 사용량과 각 메일, 에디터, 컴파일러 사용횟수 등을 들 수 있다. 서비스 거부 방법은 대표적으로 3 가지 방법이 있는데 이러한 방법을 탐지하기 위해서는 표 2 와 같은 측정치들이 필요하다.

표 2 서비스 거부 탐지에 필요한 이벤트 측정치

서비스 거부 유형	탐지에 필요한 이벤트 측정치
디스크 채우기	I/O usage, 발생한 레코드 write 이벤트 수,
메모리 고갈	CPU usage, Memory usage
프로세스 만들기	CPU usage, 발생한 Fork 이벤트 수

그 외에 메일, 에디터, 컴파일러 사용 용량 및 횟수 평가를 통해 메일 폭탄, 에디터 버그 등을 탐지할 수 있다.

다음과 같이 프로세스 관련 척도는 시스템에서 발생되는 다양한 정보들을 실시간으로 받아들여 평가를 해야 하기 때문에 평가 시간이 긴 HMM 모델을 통해서는 사용하기 어렵다. 따라서 본 논문에서는 통계적 알고리즘을 통한 분석 방법을 제안한다. 데이터는 정상행위를 통하여 구하게 되며 하나의 레코드들을 읽은 후 데이터베이스에 누적된 변수 값을 참고하여 현재 사용량이 정규분포를 통하여 정해진 임계치를 넘는지를 비교한 후 침입 시도가능 여부를 결과에 따라 Red(위험), Yellow(의심), Green(정상) 3 가지 형식으로 판단하게 된다. 결국 많은 통계자료 및 침입자를 판단하는 기준이 되는 적절한 임계치 설정이 분석 성능을 좌우하게 될 것이다.

3.3 파일 입출력 척도를 위한 상태전이 모니터링

파일 입출력 척도에서는 파일에 접속하는 주체(Suject)와 파일의(Object) 소유권한 사이에서 발생되는 상태전이를 모니터링 하게 된다. 사용되는 이벤트는 소유권한(Group ID, Effective ID, Real ID), 접근 권한(Permission mode,owner), 사용하는 프로세스 등 주로 시스템의 정보나 내부의 자원들이 중심이 되는데 이러한 탐지를 통하여 관리자나 사용자의 권한 설정 오류를 탐지 할 수 있다.

3.4 다중 척도 결과 통합을 위한 퍼지 추론

침입탐지를 위한 척도는 탐지 목적에 따라 다양하게 선택할 수 있으며, 그 중 시스템 호출, 파일 입출력, 프로세스 관련 정보는 대표적인 척도가 될 수 있다. 하지만 다양한 척도의 결과들로부터 침입을 판정하는 것은 단순한 일이 아니다. 이와 같은 다중 척도 결과를 통합하기 위해서는 각 척도의 특성을 이용하여 탐지된 결과를 적절히 조합할 수 있어야 한다.

퍼지 추론은 이러한 정량화 하기 힘든 전문가의 지식을 반영하는데 효과적인 방법으로 침입탐지를 위한 다양한 척도들의 결과값에 퍼지를 적용하여 관련된 정보를 반영한다면 더욱 정확하게 침입을 판정할 수 있을 것이다. 이러한 퍼지 방법을 구현하기 위해서는 탐지된 비정상행위의 정보에 따라 각 척도 별 탐지의 중요성을 변형시키는 최적의 Rule 을 적용시켜 비록 척도에서 서로 다른 결과를 보였다고 하더라도 오류율을 낮춰야 할 것이다.

3.5 침입 유형 결정 모듈

비정상행위 기법은 탐지된 침입유형에 대한 세부내용을 알기가 쉽지 않다. 따라서 다중 척도 분석을 통하여 생성된 정보를 기준으로 침입 유형에 대한 적절한 분석이 필요하다. 침입 유형은 호스트 기반 침입에서 발생될 수 있는 8 가지 패턴으로 구분하였으며, 탐지 후 침입으로 판정되었을 경우 각 척도 별 관련 이벤트들을 수집하여 정의된 유형의 Rule 과 비교를 통하여 분석하게 된다. 이를 통하여 각 침입에 대한 정보나 침입유형을 파악할 수 있고 보다 신뢰 있는 결과를 보여 줄 수 있다.

4. 실험 결과

본 실험에서 제안하는 침입탐지시스템은 기존 비정상행위 침입탐지 시스템들의 단점인 모델링 시 많은 시간 요구와 탐지율에 따른 False-Positive 오류를 줄이기 위해 HMM 모델링 시 권한 이동 관련 이벤트의 추출기법과 전체 데이터를 이용하여 사용하였을 때의 차이점을 비교하였다.

실험을 위해 10 명의 사용자가 참여를 하였으며, 총 수집된 데이터는 90 메가바이트이고 시스템 호출의 개수는 767,237 개이다. 각 데이터는 Solaris 운영체제 자체에서 지원하는 Basic Security Module(BSM)을 사용하여 감사자료를 수집하였다. 테스트에서는 3 명이 각 Exploit 에 대해서 2~3 번씩 침입을 시도하였다. HMM 모델의 상태값은 경험적인 연구를 통하여 5, 7, 10, 15 로 고정하였고 시퀀스 길이도 20, 25, 27, 30 으로 변화해 가며 실험하였다. 또한 정상행위 모두를 학습시켰을 때의 모델링 시간에 비해 대상을 권한이동 순간으로 하였을 때 모델링 시간이 얼마나 단축되는지에 대해서도 실험해 보았다.

4.1 정상행위 모델링 시간 측정

실험 결과 전체 학습 데이터를 이용할 경우 많은 논문에서 제기 되었던 HMM 모델의 문제점과 마찬가지로 시간이 매우 많이 소요된다는 것을 알 수 있었다. 이는 하루에도 엄청난 양의 감사자료를 발생시키는 대규모 서버에서는 학습하는데 몇 달이 걸릴 수 있고 실시간 탐지가 거의 불가능하다는 것을 의미한다. 하지만 침입의 핵심이 되는 권한 이동 순간만을 수집 모델링 했을 경우 시퀀스 개수가 약 1/132 정도로 단축되었고 이로 인해 모델링 시간 또한 약 1/256 로 단축되었다. 이 결과 권한 이동을 이용하였을 경우 얼마나 많이 시간 축약이 가능한지 알 수 있었다. 본 실험에서는 상태와 시퀀스의 길이에 따른 시간의 변화 또한 측정하였는데, 시퀀스의 길이에 따는 변화보다는 상태의 변화에 따라 시간이 차이가 많이 나는 것을 알 수 있었다. 즉 같은 탐지율을 얻을 수 있다면 상태를 최저로 하는 것이 시스템의 성능 향상에 도움이 될 것이다.

표 3 각 모델링에 대한 학습 소요시간 측정

모델링 방법	상태/시퀀스	시퀀스개수	시간
전체 데이터	5/20	767218	5 시간 07 초
전체 데이터	15/30	767208	6 시간 29 초
권한이동 데이터	5/20	5950	26.3 초
권한이동 데이터	15/30	5792	57.5 초

4.2 각 모델링 별 성능 비교

본 실험에서는 테스트 데이터 실험 시 정상행위 모델링으로부터 추출된 값을 기준으로 임계치를 조정시켜 각각의 상태에 따른 탐지 성능과 시퀀스 길이에 따른 탐지 성능을 보이기 위해 False-Positive 오류율과 침입탐지율에 대한 ROC (Receiver-Operating Characteristics) 곡선으로 그렸다. 실험 결과 전체 정보 이벤트 모델링에 비해 권한이동 관련 데이터를 이용하였을 경우 탐지율이 오히려 증가함을 볼 수 있었다.

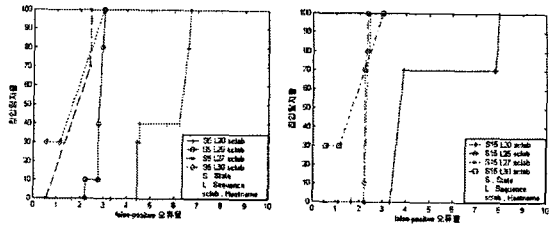

그림 4 권한이동 관련 이벤트에 대한 침입 탐지율

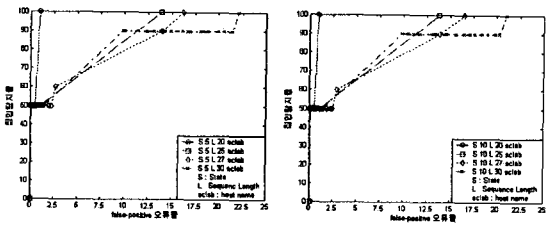

그림 5 전체 데이터에 대한 침입탐지율

5. 결론

본 논문에서는 기존 연구를 통하여 각 척도에 대한 최적의 모델링 방법을 제안하였으며 실험을 통하여 권한이동관련 데이터 추출기법이 HMM 모델의 취약점인 모델링 시간을 단축하는데 효과적임을 보였다. 또한 권한이동 이외의 DOS 공격과 같은 비정상행위를 탐지하기 위하여 제안하였던 다중 척도 결합 시스템은 지금 현재 구현 중이다. 앞으로 척도 별 결과에 대한 퍼지 추론의 적절한 침입 분석이 가능하다면 다양한 공격 패턴에 대한 모든 탐지가 가능해질것이라 사료된다.

참고문헌

[1] Endler. D. Intrusion detection: Applying machine learning to solaris audit data. In Proceeding of the 1998 Annual Computer Security Applications Conference (ACSAC"98), pages 267-279, Los Alamitos, CA, December 1998.

[2] Choy. J. and Cho. S. B., " An intrusion detection system with temporal event modeling based on hidden Markov model," *Proc. Korea Information Science Society* (B), Seoul, pp 306-308, October 1999.

[3] Warrender. C., Forrest. S. and Pearlmutter. B., "Detecting intrusion using calls: Alternative data models," IEEE Symposium on Security and Privacy, May 1999.

[4] CERT Korea Coordination center, http://www.certcc.or.kr/, 2002.

[5] Choy. J. and Cho S.-B., "Intrusion detection by combining multiple hidden Markov models," *Proceedings of The Sixth Pacific Rim International Conference on Artificial Intelligence*, August 2000.