권한 이동 이벤트를 이용한 은닉 마르코프 모델 기반 침입탐지 시스템*

박혁장 정유석 조성배
연세대학교 컴퓨터과학과
{twinkler, j8508, sbcho}@candy.yonsei.ac.kr, sbcho@csai.yonsei.ac.kr

An Intrusion Detection System Using Privilege Change Event Modeling based on Hidden Markov Model

Hyuk-Jang Park, Yoo-Suk Jung and Sung-Bae Cho
Computer Science Department, Yonsei University

요 약

침입의 궁극적 목표는 루트 권한의 획득이라고 할 수 있는데 최근 유행하고 있는 버퍼 오버플로우(Buffer Overflow) 등이 대표적이다. 최근 날로 다양화되는 이런 침입방법들에 대응하기 위해 비정상행위 탐지기법 연구가 활발한데 대표적인 방법으로는 통계적 기법과 전문가시스템, 신경망 등을 들 수 있다. 본 논문에서 제안하는 침입탐지시스템은 권한 이동 관련 이벤트의 추출 기법을 이용하여 Solaris BSM 감사 기록에서 추출된 정보 이벤트들을 수집한 후 은닉 마르코프 모델(HMM)로 모델링하여 정상행위 모델들을 만든다. 추론 및 판정시에는 이미 만들어진 정상행위 모델을 사용하여 새로 입력된 사용자들의 시퀀스를 비교 평가하고, 이를 바탕으로 정상 권한이동과 침입시의 권한이동의 차이를 비교하여 침입여부를 판정한다. 실험결과 HMM만을 사용한 기존 시스템에 비해 유용함을 알 수 있었다.

1. 서론

지난 수년간에 걸쳐, 정보 통신 기술은 가히 혁명적인 발전을 거듭하여 왔다. 우리가 알고 있듯이, 인터넷은 컴퓨터 환경을 크게 변화시켜 왔으며 가능성은 끝이 보이지 않을 정도이다. 그러나 이에 못지 않게 컴퓨터 시스템 침입에 대한 위험성도 너무나 커져 있다는 것은 부인할 수 없는 사실이다. 국내외적으로 정보시스템에 침투하여 중요 정보의 변조 및 삭제, 불법 정보 유출 등과 같은 해킹이 증가 추세에 있고 그 수법이 날로 고도화되고 있어 정보시스템에 대한 침입을 실시간으로 발견하고 보호하는 기술이 필요하다.

침입탐지 시스템은 내부자의 불법적인 사용, 오용, 또는 외부 침입자에 의한 중요 정보의 유출 및 변경을 알아내는 시스템으로써 현재의 기술적, 실제적 논점은 실제 침입이 아닌데 침입으로 판정하는 경우와 실제 침입인데 탐지하지 못하는 경우를 어떻게 처리하는가에 있다. 침입탐지 시스템은 크게 2가지로 나눌 수 있는데 첫째는 정상사용자의 행위를 모델링 하여 현재 관찰중인 사용자의 행위가 정상에서 벗어나는 지를 검사하는 비정상행위 탐지 기법과 두 번째는 기존의 공격패턴에 대한 특징 정보를 통해 똑같은 행위 시 침입으로 판정하는 오용탐지 기법이다. 오용탐지의 경우에는 기존에 잘 알려진 침입일 경우에는 높은 탐지 성능을 보이지만 잘 알려지지 않은 침입일 경우에는 탐지 할 수 없다는 단점이 있다. 비정상행위 침입탐지 시스템은 침입탐지율이 오용탐지 시스템에 비해 떨어지고 침입이 아닌 행위를 침입으로 판정하는 에러가 높지만 알려지지 않은 새로운 침입패턴에 대해서도 탐지가 가능하다는 장점을 가지고 있다.

본 논문에서는 음성인식 및 영상인식, 생명공학분야에서 알려지지 않는 대상을 모델링 하는데 쓰이고 있는 HMM을 이용하여 사용자의 정상행위 모델링을 구축하였으며 이를 기반으로 하여 새로운 데이터에 대해 비정상행위 판정을 하였다. 또한 권한 이동 관련 정보만을 추출하는 모듈을 두어 정상적으로 사용되는 권한이동을 수집한 후 실험을 통하여 비정상적인 권한이동이 있을 경우 제안한 시스템이 적절히 탐지할 수 있는지를 평가하였다.

2. 관련연구

최근 날로 다양화되는 침입방법들에 대응하기 위해 비정상행위 탐지기법 연구가 활발한데 대표적인 방법으로는 통계적 기법과 전문가시스템, 신경망 등을 들 수 있다[1]. 통계적 방법은 평상시 사용자의 패턴을 분석 후 입력 패턴과 비교하여 침입을 탐지하는 모델로써 사용자별 측정 변수를 누적한 후, 미리 정의된 임계치에 따라 침입 정도를 판별하게 된다. 전문가시스템은 주어진 기간동안 사용자의 행동을 통계적으로 기술하는 규칙 집합을 구축, 현재 활동을 이 규칙과 비교하여 비정상행위를 탐지한다. 하지만 전문가시스템 접근방식은 새로운 사용패턴을 적응시키기 위해 주기적으로 규칙베이스를 갱신해야 하는 단점이 있기 때문에 정책기반 사용 프로파일에는 유용하지만 많은 양의 감사정보를 처리하는데는 통계적인 접근방식보다 덜 효율적이다. 신경망은 새로운 입력-출력 쌍을 얻기 위해 두 집합의 정보간 관련성을 학습하고 일반화하는데 사용되는 알고리즘 기법이다. 침입탐지에서 신

* 본 논문은 (주)정보보호기술의 지원에 의한 것임

경망은 시스템내의 사용자나 데몬 등의 행위를 학습하는 것이 주된 용도이다. 신경망을 사용할 경우 통계적 기법에 비해 변수들간의 비선형적 관계를 표현하는 것이 쉽고 신경망을 자동적으로 학습시킬 수 있다. 그러나 신경망은 여전히 많은 계산을 요구하기 때문에 침입탐지분야에서는 잘 사용되지 않고 있다.

3. 권한 이동 정보를 사용한 침입탐지

침입의 궁극적 목표는 루트 권한의 획득이라고 할 수 있는데 최근 유행하고 있는 버퍼 오버플로우(Buffer Overflow) 등이 대표적인 방법이다. 이러한 침입은 사용하지 않거나 패스워드가 없는 일반 유저의 권한으로 침입을 하여 고도화된 공격 기법을 이용, 루트의 권한을 획득하게 되는데 이 때 Real User ID(UID)값과 Effective User ID(EUID)값의 차이가 생긴다. 또한 Unix 시스템에서 지원하는 C2 보안 감사를 통하여 일반적인 권한 이동과 비교, 분석을 하였을 경우 차이점을 발견 할 수 있을 것이다. 본 논문에서는 이러한 가정을 기반으로 기존의 HMM를 이용한 침입탐지에 다음과 같은 권한 이동 탐지기법을 적용시켰을 경우 기존의 시스템에 비해서 보다 낮은 Fasle-positive 에러를 얻을 수 있는지를 평가해 보았다.

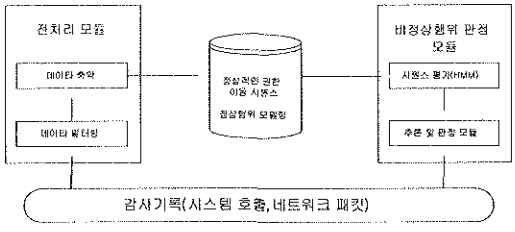

그림 1. 침입탐지 시스템 개요

3.1 감사자료의 수집 및 축약

감사자료의 수집과 축약은 침입 탐지의 첫 단계로서, 최종 목표는 아니지만 중요한 위치를 차지하고 있다[2].

권한 이동의 정보를 추출하기 위해 그림 2와 같은 SunOS의 BSM(Basic Security Module)을 사용하는데, BSM 데이터를 통하여 추출되는 막대한 양의 데이터를 이용하기 위해서는 설정 파일 조정 등을 통하여 정보의 손실을 최소화시키고 탐지에 필요한 효율적인 대표 값들을 추출하는 작업이 필요하다[3]. 본 프로그램에서는 추출된 다량의 레코드 정보 중 UID, EUID, 소유권, 시스템호출 이벤트 등을 사용하게 된다. 순서적으로 생성되는 이벤트는 일정 크기의 윈도우를 잎으로 이동시켜가면서 윈도우 크기 만한 시퀀스로 추출하였다.

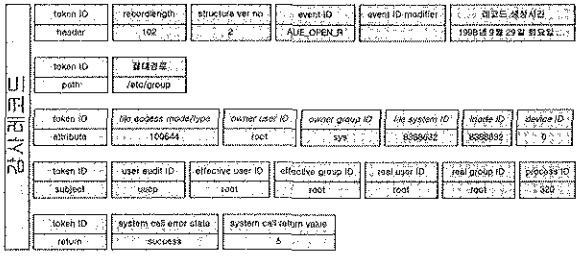

그림 2. BSM 감사 레코드

3.2 권한 이동 탐지 모듈

정상적인 권한 이동은 관리자가 일반사용자의 권한으로 들어와 작업도중 SU 명령 등을 통하여 루트의 권한을 획득하거나 일반 사용자가 잠시 루트 소유의 시스템 파일(SETUID)로 되어 있는 명령이를 실행시킬 때 발생한다. SETUID라는 것은 임시적으로 사용자의 권한을 바꿔줄 수 있는 룰을 파일에 적용시켜주는 것으로써 어떤 사람이든 SETUID로 설정된 파일을 실행하면 그 파일의 소유 계정으로 프로그램이 실행된다. 대부분의 침입은 SETUID로 설정된 파일의 버그를 이용하여 권한을 획득하게 된다. 이때 잠시 바뀌는 권한 이동 전의 행동들이 정상행위와 비정상 행위를 구분하는 중요한 시점이 되기 때문에 권한 이동을 탐지하기 위해서는 BSM Audit Data를 통하여 정상적인 권한이동에 쓰이는 정보들을 현재 시점으로부터 과거 일정한 기간동안 기록해야 한다. 기록의 범위는 임의적으로 변경하여 최적의 값을 찾게 되는데, 시퀀스의 개수를 25개미만으로 줄였을 경우 False-Positive 오류가 높아져 사용자의 권한 이동 패턴을 저장하기에 부족함을 알 수 있었고 40이상으로 설정하였을 때는 오히려 탐지율이 저하되었다. 권한이 이동되는 시점의 BSM 데이터를 분석하였을 경우 표 1 과 같은 시스템 호출 이벤트들이 발생하는데 침입이 시도되었을 경우에는 직접 실행되는 execve 이벤트 전에 symlink, setpgrp seteuid, vfork 등이 많이 발생되었다. 이러한 방법을 통해 EUID와 UID가 변경되었을 경우 그 시점을 기준으로 전에 사용되었던 일정양의 데이터 시퀀스를 따로 저장 후 각각 HMM모델에 적용시켜 기존의 HMM 기반 침입탐지 시스템과 비교하게 된다.

표 1. 권한 이동관련 이벤트

이벤트 아이디	시스템 호출	이벤트 아이디	시스템 호출
2	fork	27	setpgrp
11	chown	38	fchroot
21	symlink	39	fchown
23	execve	200	setuid
24	chroot	215	seteuid
25	vfork	6159	su

3.3 침입탐지를 위한 HMM

본 연구에서는 HMM 기반 비정상행위 탐지기법을 사용하여 침입을 탐지한다. 비정상행위 탐지를 위해서는 정상행위를 모델링하여 프로파일을 구축하는 과정과 사용자 감사기록을 판정하여 비정상여부를 가리는 과정이 필요하다.

HMM은 불완전한 관측치를 가진 이중의 확률 과정으로써 단지 생성된 시퀀스에 의해서 확률적으로 관측할 수 있다. 1960년대 말과 1970년대 초에 발표된 이 모델은 현재 음성인식과 영상인식, 생명공학분야에서 널리 쓰이고 있다. HMM는 어떤 관측 할 수 있는 시그널 과정에는 상태가 있다는 가정을 통하여 새로운 상태가 바로 전 상태에 의존하게되는 상태전이 확률과 각각의 전이가 일어난 후 관측된 심벌이 현재의 상태에 의존하는 관찰확률을 구하게 된다[4]. HMM식은 다음과 같이 표현 할 수 있으며 A와 B를 만족하는 이중확률과정을 이산형 HMM이라고 하며 기호 $\lambda = (A, B, \pi)$로 나타낸다.

정상행위 모델링은 권한 관련 정보 시퀀스를 기반으로 HMM의 매개변수를 결정하는 과정이다. HMM의 파라메터 결정은 주어진 시퀀스 O가 해당 모델 λ로부터 나왔을 확률인 $Pr(O \mid$

λ)값이 최대가 되도록 λ=(A,B,π)를 조정한다. 이를 기준으로 각각의 정상행위 시퀀스들의 평가값들을 얻게 된다.

비정상 행위 판정에서는 이미 구축되어 있는 정상행위별 HMM 매개변수에 사용자행위 시퀀스를 입력으로 넣고 각 정상행위에서 현재 행위가 생성되었을 확률을 구한다. 구해진 확률값은 기존 정상행위에서 생성된 임계값과 비교하여 비정상 행위 인지를 판정한다.

4. 실험 및 결과

학습 데이터는 일주일 동안 3명의 사용자가 발생시킨 정상행위 데이터를 사용하였다. 주 사용 프로그램은 문서편집기와 컴파일러, 그리고 사용자가 작성한 프로그램이었다. 학습 데이터에서 나온 이벤트는 모두 38433개였으며 테스트에서는 2명의 사용자가 이벤트를 발생시켰다. Attack은 19차례에 걸쳐 시도되었고 이벤트 수는 22021개였다. 이 실험에서는 최적의 성능을 보일수 있는 HMM의 매개변수를 결정하기 위한 실험도 병행되었는데, 그림 5 와 그림 6은 상태수의 변화에 따른 ROC곡선으로서 변경 가능한 매개변수의 조정에 따른 탐지율과 False-Positive의 변화를 볼 수 있다. HMM에 사용된 상태의 수는 각각 3~10로 설정하였고 시퀀스는 20~50 중 30일 때 최적의 탐지율을 나타냈다. 사용된 시스템 이벤트 수는 총 255개로 축약 없이 사용하였다. 기존 HMM모델을 사용하였을 경우 판정 모듈을 통해 나온 평가값들의 빈도는 다음 그림 3과 같고 Attack의 경우 -126을 넘어섰다. 권한 이동 탐지기법인 경우 -84를 넘어 섰다.(0에 가까울수록 정상행위 모델과 유사)

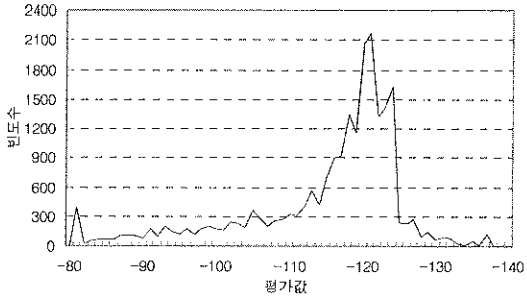

그림 3. 모든 시스템 이벤트에 대한 평가값 빈도수

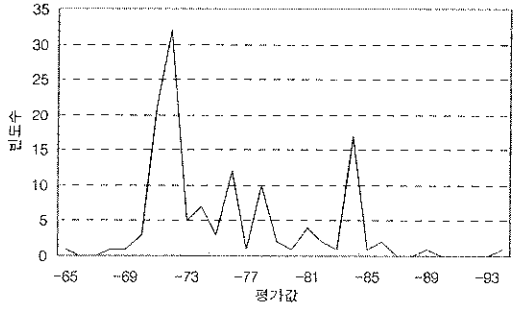

그림 4. 권한 이동 평가값 빈도수

탐지율은 기존 시스템 사용시 상태 10, 시퀀스 30에서 최적의 탐지율을 보였고 False positive error는 3.8028%일 때 침입 탐지율이 100%가 되었다. 권한 이동 탐지기법 적용시 상태 5와 7, 시퀀스는 30에서 최적의 탐지율을 보였으며 False-Positive 오류는 2.31일 때 94.7%의 탐지율을 보였다.

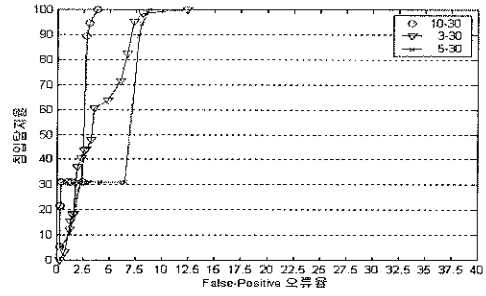

그림 5. 모든 시스템 이벤트 사용시 침입 탐지율

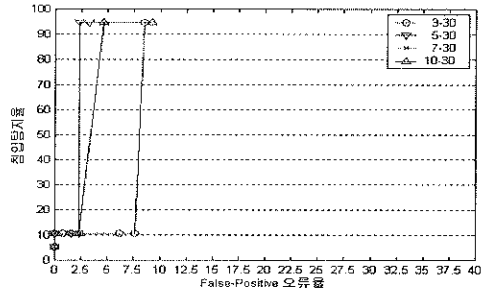

그림 6. 권한 이동 관련 침입 탐지율

5. 결론 및 향후연구

본 논문에서는 HMM를 사용한 권한 이동 탐지기법을 제안하였다. 실험 결과에서 보듯이 기존의 침입시스템에 비해 False-Positive 오류율을 줄일 수 있어 더 안정적인 판정을 내릴 수 있었다. 하지만 권한이동 탐지시 모든 평가에서 침입탐지율이 100%를 얻지 못하였는데 이는 침입이 짧은 시간에 연속적으로 일어날 경우 권한 이동 시점 이전으로부터 일정한 시퀀스만큼 데이터를 얻지 못하므로 HMM을 통한 평가가 불가능해져 발생하였다. 보다 정교한 권한이동 탐지 시스템을 위해서는 차후 시스템 호출뿐만 아니라 다른 이벤트들의 다변량 결합 등을 통하여 평가하는 작업이 필요할 것이다.

참고문헌

[1] J. Choy and S. B. Cho, "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.

[2] T. Lane and C. E. Broadly, "Temporal sequence learning and data reduction for anomaly detection," *Proc. ACCS* '98, pp. 150-158, 1997.

[3] Endler, D. "Intrusion detection. Applying machine learning to Solaris audit data," *Proceedings. Computer Security Applications Conference*, pp 268-279, 1998.

[4] L. R. Rabiner and B.H. Juang, "An introduction to hidden Markov models," *IEEE ASSP Magazine*, pp 4-16, 1986.