다중척도 모델링 및 결합을 이용한 침입탐지

한상준[0] 조성배
연세대학교 컴퓨터과학과
morello8@candy.yonsei.ac.kr[0], sbcho@cs.yonsei.ac.kr

Intrusion Detection Using Multiple Measure Modeling and Integration

Sang-Jun Han[0], Sung-Bae Cho
Dept. of Computer Science, Yonsei University

요 약

정보통신기술이 발전함에 따라 시스템 보안의 중요성이 점점 높아지고 있다. 이에 따라 내부자의 불법적인 시스템 사용이나 외부 침입자에 의한 중요 정보의 유출 및 조작을 알아내는 침입탐지시스템에 대한 연구가 활발히 이루어지고 있다. 침입탐지시스템에서는 사용자가 입력한 명령어, 네트워크 패킷, 시스템 호출 감사자료, 시스템 사용시간 등의 다양한 척도를 사용하여 침입여부를 결정하는데 사용하는 척도와 모델링 방법에 따라 취약점이 존재하여 탐지하지 못하는 침입이 있다. 본 논문에서는 단일척도 침입탐지 시스템의 취약점을 보안하기 위해 시스템 호출, 프로세스의 자원점유율, 파일접근이벤트의 세가지 척도를 각각 최적의 방법으로 모델링 한 후 결합하는 침입탐지 방법을 제안하고 실험을 통해 그 가능성을 보인다.

1. 서론

정보통신 기술의 눈부신 발전으로 점점 많은 분야에서 컴퓨터를 활용하게 됨에 따라 외부 침입자의 공격에 의한 중요정보 유출, 시스템의 불법적 사용 등에 의한 피해도 커져 시스템 보안에 대한 요구와 관심이 증대되고 있다. 실제로 한국정보보호진흥원의 보고에 따르면 2000년에는 1,943건의 국내 해킹사고가 접수되었고 2001년에는 5,333건이 접수되어 폭발적인 증가세를 보이고 있다[1]. 또한 인터넷의 대중화로 누구나 쉽게 해킹 도구를 이용할 수 있게 되어 단순한 호기심에 의한 공격도 생겨나 앞으로 해킹사고는 더욱 늘어날 전망이다.

침입탐지 시스템은 이러한 불법적인 시스템 사용에 대응하기 위한 중요한 도구중의 하나로 외부 침입자의 공격을 탐지할 수 있게 해주는 소프트웨어이다. 침입을 탐지하기 위한 기법에는 미리 알려진 공격에 대한 정보를 이용하는 오용탐지 방법과 사용자나 프로그램의 정상행위에 대한 정보를 이용하는 비정상행위 탐지 방법의 두 가지가 있다. 대부분의 상업용 침입탐지 시스템은 오용탐지 기법을 적용한 규칙기반 침입탐지 시스템이기 때문에 새로운 공격에 대한 탐지가 힘들다. 이런 오용탐지 기법의 단점보완을 위해 최근에 비정상행위기법의 침입 탐지 시스템에 관한 연구가 활발한데, 비정상행위기법의 경우에도 수집하는 정상행위 정보와 모델링 방법에 따라 탐지할 수 있는 침입의 종류가 제한적이라는 단점이 있다.

본 논문에서는 이런 침입탐지 시스템의 단점을 극복하고 탐지 성능을 향상시키기 위해 여러 가지 척도와 각 척도에 맞는 정상행위 모델링 방법을 제시하고, 단일척도 모델링 방법에 비해 좋은 성능을 보이는지를 평가한다.

2. 관련연구

대표적인 비정상행위기법의 침입탐지 방법에는 통계적 방법, 전문가 시스템, 신경망, 컴퓨터 면역시스템 등이 있다. 통계적 방법은 정상적인 사용자의 자원 사용량, 명령어 패턴, 로그인 시간의 정보 등을 통계적으로 분석한 후 입력된 정보와 비교하여 침입을 탐지한다. 신경망은 통계적 기법에 비해 비선형적 관계를 잘 표현하고 자동적으로 학습하는 장점이 있지만 계산량이 많고 입력과 출력간의 관계를 알 수 없는 단점이 있다. 전문가 시스템 방법은 정상적인 사용자의 기록으로 사용자의 행동을 기술하는 규칙집합을 만들고 입력된 정보를 비교하여 침입을 탐지한다. 이 방법은 주기적으로 규칙정보를 재구성해야 하기 때문에 많은 양의 감사정보를 처리하기에는 무리가 따른다. 면역 시스템은 사용자가 아닌 서비스의 정상행위를 모델링하는 것으로 수집된 데이터가 포괄적이라면 낮은 오류율을 보이지만 합법적인 행동으로 불법 접근하는 것을 막을 수 없다.

3. 다중척도기반 침입탐지

본 논문에서는 정상행위에서 얻어지는 여러 가지의 척도를 얻어내고 각 척도에 맞는 최적의 모델링 방법을 선택하여 정상행위를 모델링한다. 이렇게 만들어진 각 모델에 대하여 취약성을 분석한 후 이를 보완하기 위해 여러 모델의 평가 값을 결합하는 규칙을 만든 후 이에 따라서 침입여부를 판정하도록 하였다. 시스템의 자세한 구조는 그림 1과 같다.

3.1 시스템 호출 척도

솔라리스의 BSM(Basic Security Module)에서 나오는

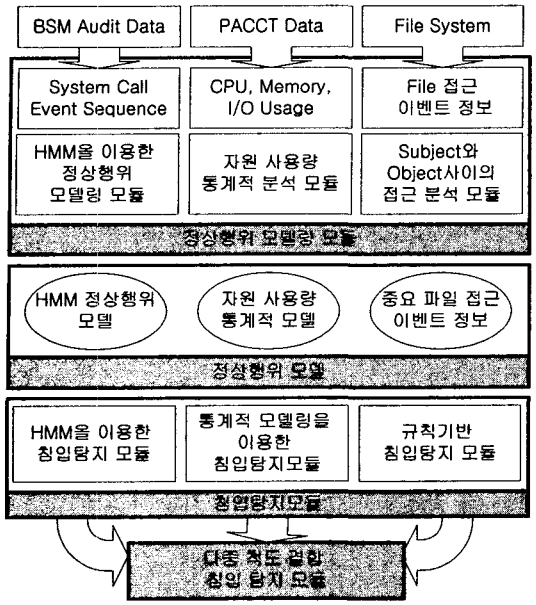

그림 1. 침입탐지시스템 구조

감사데이터는 운영체제에서 발생한 시스템 호출 이벤트들과 그에 관련된 사용자 및 프로세스 정보를 포함하는 자료로 침입탐지 시스템에서 가장 많이 쓰이는 척도이다. 본 논문에서는 시스템 호출 감사 정보를 모델링하기 위하여 음성인식과 영상인식 등의 분야에서 널리 쓰이는 HMM(Hidden Markov Model)을 사용하였다. HMM은 실제적인 생성경위를 알기 힘든 이벤트 시퀀스를 잘 모델링할 수 있는 방법으로 시스템 호출 감사 자료를 모델링하는데 유용한 도구이다[2].

HMM은 초기상태 확률분포 π 와 상태전이 확률분포 A, 관측기호 확률분포 B로 구성되는데 기호로는 λ = (A, B, π)로 나타낸다. 정상행위 모델링은 구축된 모델로부터 주어진 시퀀스 O가 나올 수 있는 확률 값인 P(O|λ)가 최대가 되도록 HMM의 구성요소들을 조정해 나가는 과정인데 이렇게 생성된 모델에 침입이 들어있는 시스템 호출 감사자료를 입력하고 정상행위 모델에서 입력된 행위가 나올 확률 값을 구해 평가한다. 이 확률 값이 정상행위 모델링에서 구한 임계값보다 낮게 나올 경우 침입으로 판정한다.

3.2 프로세스 척도

대부분의 운영체제에서 감사자료로 사용되는 PACCT(Process Account)자료는 프로세스의 CPU점유율, 메모리 사용량, I/O사용량 등의 정보를 제공한다. 일반적으로 시스템의 자원을 모두 고갈시켜 마비시키는 DoS(Denial of Service)공격의 탐지에 유용한 자료이다. 본 논문에서는 정상적인 프로세스가 남긴 PACCT 감사자료를 통계적 방법으로 분석하여 정상행위의 프로파일을 만든 후 입력된 감사자료의 분석 값과 비교해 침입을 판정하였다.

통계적 분석방법은 기존 NIDES[3]에서 사용된 방법을 기반으로 DoS공격을 탐지할 수 있도록 수정하여 사용하였다. Q통계치는 현재의 자료와 과거의 자료 사이의 유사성을 판단하는 기준으로 근래의 자료에 가중치를 두어 오래된 자료일수록 통계 값에 영향을 덜 미치도록 한 것이다. D_k를 k번째 자료와 k+1번째 자료 사이의 변화량이라 하고 t_k는 마지막에 들어온 자료와 k번째 자료 사이의 시간, r을 최근 자료의 가중치라고 할 때 Q통계치는 다음 공식으로 얻을 수 있다.

$$Q = \sum_{k \geq 1} D_k \times 2^{-rt_k}$$

이러한 공식에 의하여 정상행위 자료에 대한 Q통계치를 얻어낸 후 이 값을 미리 정해놓은 구간에 대응시켜 정상행위의 Q값이 각 구간에 속할 확률을 구한다. 이 확률을 누적 정규 분포표에 대응시켜 각 구간에 대한 최종 평가 값을 구하는데 이 값을 S라고 한다.

표 1. 각 구간별 자원 사용 평가값(S값) 분포

	1	2	3	4	5	6	7
CPU	0.0	0.03	0.07	0.15	1.26	3.78	20.02
Mem.	0.0	1.0	3.0	5.0	7.5	10.5	12.0
I/O	0.0	1.5	2.0	3.0	4.0	5.0	6.0

이렇게 정상행위 자료에서 얻어진 각 구간별 S평가 값은 침입 판단의 기준이 되는데, 테스트 자료의 Q평가 값이 속한 구간의 S값이 그 자료의 평가 값이 된다. PACCT 레코드의 각 척도 별로 구해진 S값에 가중치를 두어 결합하여 구해진 하나의 레코드에 대한 최종 평가 값을 T라하고 이 T값으로 침입여부를 결정한다. T값은 s_n을 각 척도별 평가 값, a_n을 각 척도별 가중치라고 했을 때 다음 공식에 의하여 구해진다[4].

$$T = a_1 s_1 + a_2 s_2 + \ldots + a_n s_n$$

3.3 파일 접근 척도

파일 접근에서 주가 되는 3가지 요소는 주체(Subject)인 프로세스 또는 사용자와 객체(Object)가 되는 파일 그리고 둘 사이에 일어나는 접근(Access)이벤트이다. 파일 접근을 활용한 대표적인 규칙은 Bell과 LaPadula의 BLP 모델을 들 수 있는데 낮은 레벨을 가지는 주체가 높은 레벨의 객체에 접근하는 것을 제한 하는 방법으로 간단히 No Read Up rule이라고도 한다[5].

본 논문에서는 이를 응용하여 파일 접근 이벤트를 모니터링하였는데 모든 파일을 모니터링하기에는 무리가 따르므로 공격의 주 대상이 되는 실행시에 root권한을 얻을 수 있는 SETUID파일만으로 대상을 줄였다. 낮은 레벨의 주체가 SETUID파일을 접근할 때에는 위험도를 높임으로써 보다 정확한 침입탐지를 할 수 있게 하였다.

3.4 다중척도 결합

침입탐지를 위한 척도는 다양한 것들이 사용될 수 있지만 각 척도의 특성과 모델링 방법에 따라 잘 탐지할 수 있는 침입이 있고 그렇지 못한 것이 있다. 본 논문에서는 표 2에서 와 같이 각 척도의 단점을 서로 보완할 수 있도록 특성을 고려하여 탐지된 결과를 조합하는 최적의 규칙을 생성하였다.

4. 실험 결과

본 논문의 실험에서는 먼저 단일 척도 탐지방법을 수행하여 그 취약점을 분석하고 이를 보완하기 위한 다중척도 결합 방법을 실행해 그의 성능향상을 알아 보았다.

시스템 호출 척도에서는 BSM감사자료로부터 HMM을

표 2. 다중 척도 결합 규칙

번호	조건	결과
1	(시스템호출평가값 < 임계값) AND (프로세스==SETUID AND Subject레벨<Object레벨)	Buffer Overflow 공격
2	(fork이벤트수/초 > 150회/초) AND (CPU점유평가값<0.3 AND I/O점유 평가값 < 1.5)	Process 만들기 DoS공격
3	(memory점유평가값>2.33 AND CPU점유평가값>2.5) AND (시스템호출이벤트수 < 5)	Memory 채우기 DoS공격

이용하여 정상행위모델을 생성하고 침입발생이 있는 감사자료를 이용+해 성능을 평가하였다. 정상행위를 모델링하기 위해 6명의 사용자가 보름 동안에 16,470개의 명령어를 입력하여 발생한 160,448개의 이벤트가 수집된 13메가바이트의 감사자료가 사용되었으며, 테스트 자료로는 6번의 버퍼오버플로우(Buffer Overflow)공격이 들어있는 자료를 사용하였다. 최적의 결과를 얻기 위해 HMM의 상태수와 시퀀스길이를 변화시키면서 실험을 반복하였고 그에 따른 결과는 그림 2와 같다.

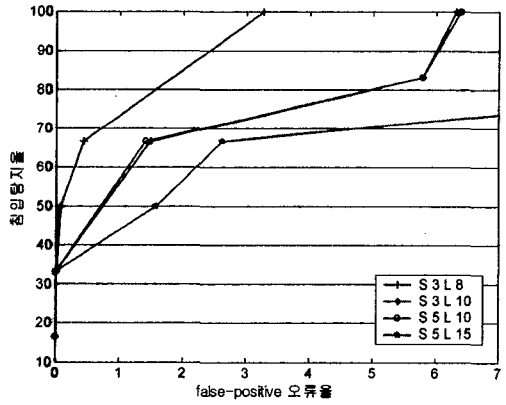

그림 2. 시스템 호출 척도 침입탐지 결과

상태수 3, 시퀀스길이 8일 때 false-positive(f-p)오류율이 3.26652%로 가장 좋은 성능을 나타내었다. 상태수보다는 시퀀스길이에 많은 영향을 받았는데 시퀀스길이가 너무 길어질 경우 f-p오류율이 급격히 증가하였다.

같은 감사자료를 이용하여 다중 척도 결합모델을 적용해보았다. 파일 접근 척도를 결합한 규칙 1을 사용하여 실험한 결과 f-p오류율이 현저히 낮아졌다. 이는 대부분의 버퍼오버플로우 공격이 SETUID프로그램을 대상으로 하기 때문이다.

프로세스 척도에서는 16,470개의 명령어에서 수집된 840킬로바이트의 PACCT감사 자료를 정상행위자료로 사용하였다. 테스트 자료는 프로세스 만들기, 메모리 채우기, 디스크 채우기 등의 DoS공격을 총 6차례 수행하여 얻어진 데이터를 사용하였다. 각 척도별 가중치를 변화시키면서 최적의 가중치를 찾아내고자 하였는데 CPU점유율에 큰 가중치를 주는 것이 좋은 결과를 보였다. 이는 DoS공격이 다른 척도보다 CPU점유율에서 정상행위와

표 3. 시스템 호출 척도와 파일접근척도 결합 결과

상태/시퀀스	임계값	탐지율	F-P오류율	결합후 F-P오류율
3/8	-19.5	100%	3.26652%	0%
3/10	-13.7	100%	6.3197%	0%
5/10	-13.8	100%	6.39405%	0%
5/15	-15.2	100%	17.7612%	0%

더 많은 차이를 보이기 때문이다. 하지만 프로세스 만들기 공격의 경우에는 탐지가 어려웠는데, 이는 자원 사용률이 낮은 수많은 프로세스로 운영체제의 프로세스 테이블을 채우는 공격이기 때문에 자원 사용량만으로는 정상행위와 구분하기 어렵기 때문이었다.

시스템 호출 척도가 결합된 규칙 2와 3을 적용하여 실험을 반복한 후 정해진 임계값에서 결합 전후의 성능 차이를 비교하였다. 표 4에서와 같이 탐지할 수 없었던 프로세스 채우기 공격도 탐지하여 탐지율을 높일 수 있었고 f-p오류율도 낮출 수 있었는데 이는 프로세스 공격이 단시간에 수많은 fork()시스템 호출 이벤트를 발생시키기 때문이다.

표 4. 프로세스 척도와 시스템 호출 척도 결합 결과

가중치 (C/M/I)	임계값	결합전		결합후	
		탐지율	F-P 오류율	탐지율	F-P 오류율
3.5/0.7/0.3	10.29	83.3%	1.786%	100%	0.893%
3/1.5/0.3	8.986	83.3%	3.571%	100%	2.679%
3/1/0.5	9.365	83.3%	2.679%	100%	1.786%
2/1/0.3	4.72	83.3%	3.571%	100%	2.679%

5. 결론

본 논문에서는 침입탐지시스템에 쓰일 수 있는 세가지 척도에 대한 모델링 방법을 제시하고 각 척도별 취약점을 보완하기 위하여 규칙기반의 다중척도 결합 방법을 이용하여 성능이 향상될 수 있음을 보였다. 하지만 좀더 다양한 척도를 분석하여 이용하고 여기서 사용한 고정된 규칙 집합에서 벗어나 탐지된 비정상행위의 정보에 따라 각 척도별 가중치를 유연하게 변화시켜 최적의 결합 규칙을 적용할 수 있도록 한다면 더욱 정확한 탐지가 가능할 것이다.

6. 참고문헌

[1] Korea Computer Emergency Response Team Coordination Center, http://www.certcc.or.kr, 2002.

[2] A.G. Amoroso, *Fundamentals of Computer Security Technology*, PTR Prentice Hall, New Jersy, 1994.

[3] H.S. Javitz and A. Valdes, The SRI IDES statistical anomaly detector, 1991.

[4] L.R. Rabiner, "A tutorial on hidden Markov models and selected applications in speech recognition," *Proc. of the IEEE*, vol. 77, no. 2, pp. 257-286, 1989.

[5] 박혁장, 침입탐지 시스템의 성능향상을 위한 다중척도 모델링기법 연구, 연세대학교 석사학위논문, 2002.