정상행위 모델링을 통한 침입탐지 시스템에서 BSM 감사기록의 효과적인 축약

서 연규, 조 성배
연세대학교 컴퓨터과학과

Effective Reduction of BSM Audit Data for Intrusion Detection System by Normal Behavior Modeling

Yeon-Gyu Seo and Sung-Bae Cho
Computer Science Department, Yonsei University

요 약

정보시스템의 보호를 위한 침입탐지의 방법으로 오용탐지와 비정상행위 탐지방법이 있다. 오용탐지의 경우는 알려진 침입패턴을 이용하는 것으로 알려진 침입에 대해서는 아주 높은 탐지율을 나타내지만 알려지지 않은 침입이나 변형패턴에 대해서는 탐지할 수 없다는 단점이 있다. 반면 비정상행위 탐지는 정상행위 모델링을 통해 비정상패턴을 탐지하는 것으로 알려지지 않은 패턴에 대해서도 탐지할 수 있는 장점이 있는데 국내외적으로 아직까지 널리 연구되어있지 않다. 본 논문에서는 BSM으로부터 얻은 다양한 정보를 추출하고 이러한 정보를 자기조직화 신경망을 이용하여 축약함으로써 고정된 크기의 순서정보로 변환하는 방법을 제안한다. 이렇게 생성된 고정크기의 순서정보는 비정상행위 탐지에 효과적으로 사용될 수 있을 것이다.

1. 서론

침입탐지의 방법은 기존의 알려진 침입패턴을 저장하고 사용자의 행동패턴과 비교함으로써 침입을 탐지하는 오용탐지와 사용자의 정상행위패턴을 이용한 비정상행위 탐지로 나누어 볼 수 있다[6]. 후자의 방법은 정상행위에 대한 프로파일을 작성한 후 침입탐지시에 저장된 정상행위 프로파일과 현재 사용자의 행동패턴과의 유사성을 비교함으로써 침입의 여부를 확인한다. 비정상행위 탐지의 경우 알려지지 않은 침입패턴에 대해서도 탐지가 가능하기 때문에 최근 관심이 고조되고 있으며 관련분야에서 많은 연구가 이루어지고 있다. 대부분의 연구들은 프로파일의 생성에 관한 문제를 다루고 있으며 통계적 기법에서부터 인공지능적인 기법(에이전트, 유전자 알고리즘, 신경망)에 이르기까지 다양한 방법이 시도되고 있다.

시스템에서 침입을 탐지하기 위해서는 시스템에서 발생하는 이벤트와 로그정보 및 프로세스 등에 대한 정보가 필요한데, 이러한 정보들은 분산되어 있거나 중복되어 있기 때문에 효과적으로 수집하기가 쉽지 않다. 이를 위해 자료수집의 방법으로 SUN에서는 커널 수준에서 각종 이벤트에 대한 기록을 남길 수 있도록 BSM(Basic Security Module)을 제공하고 있다. BSM은 호스트에서 발생하는 로그나 프로세스, 이벤트에 대한 다양한 감사기록을 남긴다. 실시간 침입탐지를 위해서는 BSM이 제공하는 다양한 많은 정보로부터 침입탐지에 필요한 정보들을 추출하고 이를 축약할 필요가 있다.

본 논문에서는 BSM감사기록에서 가능한 여러가지 정보를 추출한 후, 입력되는 패턴에 따라 자기 조직화하여 유사한 패턴으로 분류해주는 자기조직화 신경망(Self-Organizing Map : SOM)[3]을 이용하여 다양한 정보들을 대표 값으로 축약함으로써 침입탐지시스템에서 정상행위 모델링을 위한 순서화된 정보로 사용될 수 있도록 한다.

2절에서는 관련연구에 대해 설명하고 3절에서는 BSM에 대해 간단히 설명을 한다. 4절에서는 BSM에서 얻은 다양한 정보를 이용하여 하나의 고정크기를 갖는 순서정보로 변환하는 과정과 축약의 방법으로 사용되는 자기조직화 신경망에 대해 알아본다. 5절에서는 다양한 실험을 통해 BSM감사기록이 SOM을 통해 효과적으로 축약됨을 보이고 마지막으로 결론을 맺는다.

2. 관련연구

최근 비정상행위 탐지에 대해 많은 연구가 이루어지고 있는데 이러한 시스템들은 대부분 사용자별로 프로파일을 작성[4, 5]하거나 프

침입탐지 시스템	데이터 소스			모델		특성
	호스트	멀티 호스트	네트웍	비정상행위	오용	
NADIR			•	•	•	규칙기반 전문가 시스템
NIDES		•		•	•	
MIDAS		•		•	•	전문가 시스템
ISOA		•		•	•	
CMDS		•		•	•	규칙기반 전문가 시스템
NID			•	•	•	

표 1. 비정상행위 탐지 시스템

로그램별로 프로파일을 작성하는 방법[1]을 사용한다. 이때, 프로파일의 생성을 위하여 BSM에서 제공하는 여러 정보와 네트워 패킷, 명령어 등을 시스템에서 지정한 포맷으로 변환한다.

프로파일을 생성하기 위한 데이터 추출을 위하여 통계적인 기법[2]을 이용하기도 하고 사용자의 행동패턴을 클러스터링하여 저장하는 방법[1, 4, 5]도 사용한다. 표 1은 기존의 비정상행위 탐지 시스템들을 보여주고 있다[7].

3. BSM(Basic Security Module)

BSM은 각종 이벤트에 대한 감사기록을 생성하고 관리한다. audit_event에서 각 이벤트에 대한 정의를 하고 이들을 유사한 것들끼리 묶어 audit_class에서 분류하여 감사할 모든 이벤트를 일일이 지적하지 않고 클래스 단위로 사용할 수 있도록 한다. 또한 audit_control에서 감사적용 범위와 대상에 대해 기록하고 있으며 audit_user에서 각 사용자별로 감사적용범위를 결정할 수 있도록 한다. 그림 1은 BSM이 감사기록을 남기는 과정에 대해 보여주고 있다.

BSM에서 얻어지는 감사기록은 그림 2와 같이 여러 감사레코드들의 묶음으로 이루어져 있다. 하나의 이벤트에 대해 기록되는 정보의 양은 그대로 이용하기엔 방대하기 때문에 실제 사용을 위해선 필요한 정보를 추출하는 과정이 필요하다.

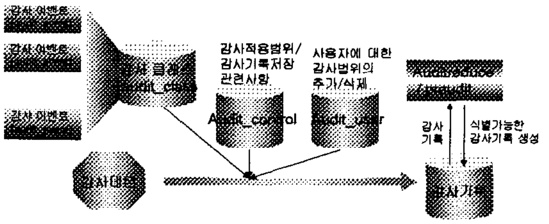

그림 1. BSM감사기록의 생성과정

token ID	record length	structure ver no	event ID	event ID modifier	레코드 생성시간
header	102	2	AUE_OPEN_R		1998년 9월 29일 화요일 ...

token ID	절대경로
path	/etc/group

token ID	file access mode/type	owner user ID	owner group ID	file system ID	inode ID	device ID
attribute	100644	root	sys	8388632	729476	0

token ID	user audit ID	effective user ID	effective group ID	real user ID	real group ID	process ID	session ID	terminal ID
subject	uucp	root	root	root	root	320	320	0 0 0.0.0.0

token ID	system call error status	system call return value
return	success	5

그림 2. BSM에서 유지하는 감사레코드들

4. 감사기록의 축약

BSM감사기록[6]에는 침입을 탐지할 수 있는 많은 양의 정보들(로그정보, 시스템 호출, 프로세스 정보)이 포함되어 있다. BSM이 남기는 감사기록은 방대할 뿐만 아니라 중요하지 않은 정보들도 포함하고 있기 때문에 실시간으로 침입을 탐지하기 위해선 중요한 정보들만을 추출하고 이때 얻어진 다차원 정보를 일차원 정보로 변환할 필요가 있다. 이 때 BSM에서 얻을 수 있는 정보는 다양한데 정보를 추출하는 방법으로는 통계적인 방법이나 전문적인 지식이 사용될 수 있다. 다차원 정보를 일차원 정보로 변환하기 위해서는 통계적인 방법이 사용되지만 여기서는 입력패턴에 따라 자기조직화하여 이차원상의 대표 값으로 출력해주는 SOM을 이용한다.

본 논문에서 사용하고 있는 비교사학습(unsupervised learning) 신경망인 SOM은 다차원 입력벡터를 Euclidean distance와 같은 유사도 측정을 통해 자기조직화하고 입력 값에 가장 가까운 대표 값으로 출력해준다. SOM의 일반적인 학습 알고리즘은 다음과 같다. 수식에서 $i(\mathbf{x})$는 입력에 가장 잘 일치하는 값이며, Λ_i는 Neighborhood 함수, η는 학습률을 의미한다.

1. 가중치 벡터들($\mathbf{w}_j(0)$)의 초기화 (n=0).
2. 유사도 비교.

$$i(\mathbf{x}) = \arg\min_j \|\mathbf{x}(n) - \mathbf{w}_j\|$$

3. 가중치 벡터들의 갱신.

$$\mathbf{w}_j(n+1) = \mathbf{w}_j(n) + \eta(n)\Lambda_{i(\mathbf{x})}(n,j)\left(\mathbf{x}(n) - \mathbf{w}_j(n)\right)$$

4. 조건을 만족할 때까지 2 ~ 4반복

BSM의 여러 Measure중에서 수치화될 수 있는 정보로서 사용자 ID, 시스템호출, 파일시스템, 파일 접근모드, 세션ID, 인자길이를 입력으로 이용하였다. 이러한 정보들 중에는 희소 사용분포를 나타내는 것이 있다. 시스템 호출의 경우 기록이 가능한 시스템 호출은 300여개 정도인데 실제로 자주 사용되는 시스템 호출의 개수는 50개 정도이다. 따라서 이러한 빈도 정보를 이용하면 작은 크기의 벡터로 축약시킬 수 있다. SOM의 입력벡터로 사용할 때 유의할 점은 SOM에서 유사도 평가기준으로 Euclidean distance를 사용하기 때문에 BSM에서 추출한 정보에서 큰 폭으로 변하는 정보들은 유사도 평가에 큰 영향을 준다는 점이다. 따라서 SOM의 입력으로 이러한 정보를 사용하기 위해서 입력벡터들의 크기를 조정해야하는데 중요하지 않은 특정 수치에 좌우되지 않도록 중요도에 따라 입력 값의 크기를 다르게 하였다.

5. 실험 결과

SOM에서의 반복회수는 100,000으로 하였으며 학습률은 0.02, 반경은 2로 하여 실험하였다. 학습과 평가를 위해 사용된 데이터는 BSM감사레코드로부터 추출된 1000개의 이벤트이다. 이때, SOM에서 맵의 크기 결정이 중요한데 BSM감사기록에서 추출된 자료들이 어떤 값으로 나와야 하는지는 알 수 없기 때문에 맵의 크기 결정을 위해 맵의 크기변화에 따른 양자화 에러(Quantization error)와 맵의 사용률을 실험으로 알아보았다. 그림 3에서 알 수 있듯이 SOM에서 맵의 크기가 증가할수록 양자화 에러 값이 줄어들지만 맵의 크기가 증가하게 되면 그림 4와 같이 사용되지 않는 영역이 늘어나게 되므로

사용되지 않는 영역이 작으면서 양자화 에러 값이 작은 맵을 선택하는 것이 중요하다.

그림 3을 보면 맵의 크기가 30이후로 거의 완만한 기울기를 보이고 있다. 그림 4는 이때의 사용되지 않은 영역의 확률을 보여주고 있는데 두 그림을 통해 적당한 맵의 크기는 30 ~50에서 선택하는 것이 좋음을 알 수 있다.

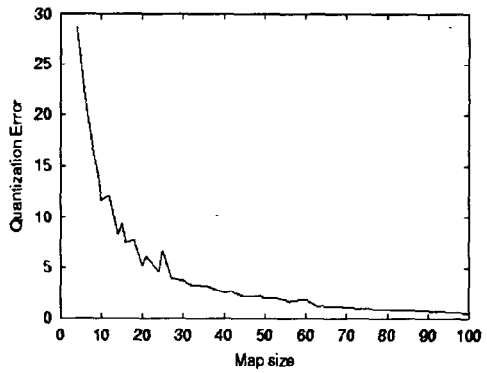

그림 3. 양자화 오류 변화.

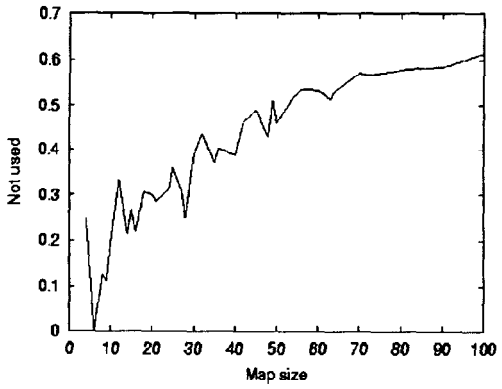

그림 4. 맵의 크기 증가에 따른 사용도 변화

6. 결론 및 향후연구

본 실험에서는 BSM에서 사용할 수 있는 여러 정보 중에서 중요하게 여겨지는 수치정보를 추출하고 SOM을 이용하여 하나의 고정크기를 갖는 순서정보로 변환하였다. 변환된 순서정보들은 적절한 방법을 통해 분할함으로써 다양한 통계적인 방법이나 인공지능적 기법에 의해 정상행위 모델링의 중요한 정보로 사용될 수 있을 것이다.

본 논문에서 사용하고 있는 BSM정보는 수치정보들만을 사용하고 있는데 수치 정보이외에 여러 정보들을 사용할 수 있을 것이다. 그리고 현재 호스트 기반 침입탐지를 위해 BSM을 사용하고 있지만 네트웍 패킷 분석을 위해서 tcpdump로부터 추출된 정보를 추가한다면 침입탐지에 더 효율적인 순서정보를 생성할 수 있을 것이다.

참고문헌

[1] A.K. Ghosh, A. Schwartzbard and M. Schatz, "Learning program behavior profiles for intrusion detection," *Proc. of WIDNM'99*, 1999.

[2] H.S. Javitz and A. Valdes, "The SRI IDES statistical anomaly detector," *Proc. of IEEE Symposium on Research in Security and Privacy*, 1991.

[3] T. Kohonen, Self-Organizing Maps, Springer press, 1995.

[4] T. Lane and C.E. Broadly, "Temporal sequence learning and data reduction for anomaly detection," *Proc. of ACCS'98*, pp. 150~158, 1998.

[5] T. Lane and C.E. Broadly, "An application of machine learning to anomaly detection," *Proc. of NISSC'97*, pp. 366~380, 1997.

[6] 한국 정보보호센터, *호스트 기반 실시간 침입탐지 시스템 개발을 위한 SunSHIELD Basic Security Module의 분석*, 1998.

[7] 한국 정보보호센터, *실시간 네트워크 침입탐지 시스템*, 1998.