데이터 마이닝 에이전트를 적용한 침입 탐지 시스템 설계

정종근* ,구제영, 김용호, 오근탁, 이윤배

조선대학교 전자계산학과*

Design of Intrusion Detection System applying for data mining agent

Jong-Geun Jeong , Je Young Koo, Young-Ho Kim , Guan-Tack Oh , Yun-Bae Lee

Dept. of Computer Science, Graduate School, Chosun Univ.*

요 약

침입 탐지 시스템은 침입 판정과 감사 데이터(audit data) 수집 분야에서 많은 연구가 진행되고 있다. 침입 판정은 주어진 일련의 행위들이 침입인지 아닌지를 정확히 판정해야 하고 감사 자료 수집에서는 침입 판정에 필요한 데이터만을 정확히 수집하는 능력이 필요하다. 최근에 이러한 문제점을 해결하기 위해 규칙기반 시스템과 신경망 등의 인공지능적인 방법들이 도입되고 있다. 그러나 이러한 방법들은 단일 호스트 구조로 되어있거나 변형된 침입 패턴이 발생했을 때 탐지하지 못하는 단점이 있다. 따라서, 본 논문에서는 분산된 이기종 간의 호스트에서 사용자의 행위를 추출하여 패턴을 검색, 예측할 수 있는 데이터 마이닝 에이전트를 적용하여 실시간으로 침입을 탐지하는 방법을 제안하고자 한다.

ABSTRACT

IDS has been studied mainly in the field of the detection decision and collecting of audit data. The detection decision should decide whether successive behaviors are intrusions or not , the collecting of audit data needs ability that collects precisely data for intrusion decision. Artificial methods such as rule based system and neural network are recently introduced in order to solve this problem. However, these methods have simple host structures and defects that can't detect transformed intrusion patterns. So, we propose the method using data mining agent that can retrieve and estimate the patterns and retrieval of user's behavior in the distributed different hosts.

Ⅰ. 서 론

침입 탐지 시스템은 단일 호스트 기반의 중앙 집중형과 다중 호스트 기반의 완전 분산형으로 나눌 수 있다. 단일 호스트 기반의 침입 탐지 시스템은 중앙 제어 시스템이 모든 서버 시스템의 감사 데이터를 전송 받아 침입을 탐지하기 때문에 통신양이 증가하고 중앙 호스트에 과부하를 주는 단점이 있다[29]. 다중 호스트 기반의 침입 탐지 시스템은 하나의 호스트에서 전체 시스템을 감시하지 않고 각 호스트가 독립적으로 침입을 탐지한다. 이와 같은 침입 탐지에 대한 다양한 기법들과 모델들이 개발되고 있으나 컴퓨터 시스템의 복잡성과 시스템 자체의 보안 취약성 그리고 새로운 침입 기법의 개발 등으로 인해 기존의 탐지 방법들은 불완전한 요소를 가지고 있다. 시스템에서 사용 패턴의 다양화 때문에 비정상 행위 탐지 IDS를 구현하는 것은 오용 탐지 IDS를 구현하는 것보다 많은 어려움이 있다. 따라서, 상용화되어 있는 대부분의 IDS는 오용 탐지 방법에 의한 것이다. 그러나, 이러한 오용 탐지 방법에 의한 IDS는 새로운(변형된) 침입 패턴이 발생할 경우 탐지해내지 못한다는 단점을 가지고 있다.

따라서 본 논문에서는 분산 환경에서 호스트 기반의 중앙 집중형과 분산형을 혼합한 하이브리드(Hybrid) 형태의 침입 탐지 시스템을 제안한다. 이를 위해 분산 환경에서는 감시 대상 시스템에 설치되어 있는데이터 마이닝 에이전트를 통해 발생하는 이벤트를 모니터링하여 침입을 판단한다. 그리고 각 호스트에서 분석된 감사 데이터를 호스트들간에 공유하도록 하며, 새로운 침입 패턴(또는 변형된 침입 패턴)이 발생할 경우 탐지해낼 수 있는 지능형 침입 탐지 방법을 제안하고 그 타당성을 입증한다.

II. 데이터 마이닝 학습

연관 규칙은 어떤 사건이 발생할 때 다음에 발생하는 사건이 서로 연관되어 있는 것을 말한다. 다시 말해서 트랜잭션 집합 X, Y가 있을 때 X→Y로의 진행에서 트랜잭션 X에 있는 임의의 항목 집합이 발생할 때 트랜잭션 Y에 있는 임의의 항목 집합도 함께 발생한다는 의미이다. 연관 규칙의 이러한 속성을 이용하여 기존에 존재하는 침입의 유형을 분석하고 기존 침입 패턴의 응용을 예측, 분석하는 기법을 제안하고자한다.

본 논문에서는 데이터마이닝을 이용한 침입정보를 분석하기 위해 setuid를 포함하고 있는 버그 중에서 /bin/mail을 이용하여 root의 권한을 획득하려고 할 때 사용되는 명령어들을 로그 데이터로 수집하여 연관 규칙을 적용한다. 메일을 주고 받거나 편집할 때 root 권한으로 /tmp에 임시파일을 생성하게 되는데 다음과 같은 과정으로 root 권한을 획득한다. 그림 1은 /bin/mail 공격의 순서를 나타낸 것이다.

```
% cc -o mailrace mailrace.c
% cat tmphost
% chmod 755 tmpmail.sh
% tmpmail.sh tmphost /.rhosts
% rsh hostname -l root sh -i
# whoami
root
```

그림 1. /bin/mail 공격 순서

표 1은 /bin/mail를 이용하여 root의 권한을 획득하기 위해 사용되는 명령어들에 대한 대응표이다.

표 1 초기 DB 명령 대응표

명령 유형	id	cc	cat	chmod 755	cd	rsh	whoami
대응값	A	B	C	D	E	F	H

/bin/mail을 사용하여 root 권한을 획득하는 순서는 다양하기 때문에 유사한 접근 시도를 유형별로 분석하여 알려진 침입 방법인지 새로운 유형의 침입 방법인지를 판별한다. 표2는 setuid를 이용한 root shell 획득을 접근 유형을 각 사용자의 접근 명령별로 나타낸 것이다.

표 2. /bin/mail 사용 유형

상태 / ID	S1	S2	S3	S4	S5
jkcom	A	B	C	D	F
yblee	B	C	A	D	F
psbum	C	F	H	B	A
yhkim	B	D	E	C	H

여기서 지지도와 신뢰도의 임계값(threshold)을 2로 주었을 때 다음과 같은 최종 감사 데이터를 생성해 낸다. 여기에서 임계값을 조정함으로 침입 패턴 순서의 변형까지 탐지할 수 있다.

표 3. 감사 데이터 생성

명령순서	B, C, D, F
빈도수	2

마지막으로 생성된 감사 데이터는 침입 패턴 데이터베이스에 저장되어 이와 같은 패턴이 발생할 때 이를 탐지한다.

III. 에이전트

침입 탐지 시스템들은 하나의 통합된 단일 호스트 기반의 형태를 가지고 있다. 이러한 시스템들은 전체 시스템에 걸리는 부하문제, 탐지 모듈의 에러문제, 시스템 확장에 따른 성능 저하 문제 등이 제기되고 있다. 이러한 문제점을 해결하기 위한 방법으로는 탐지 시스템을 기능적, 독립적으로 분할하는 에이전트를 채용해서 다수의 프로세스들로 하여금 각각 독립적인 동작으로 분할된 시스템들을 모니터링 한다. 에이전트는 감사 데이터를 수집하여 시스템에 침입이 발생할 경우 에이전트들 간의 협력을 통해서 침입을 탐지하고 대응하는 핵심 요소라고 할 수 있다. 에이전트는 다른 에이전트와 상호간의 통신이 가능하며, 침입 탐지 에이전트를 생성한 메인 호스트가 네트워크를 제거하기 전까지 활동을 할 수 있어야 한다. 이러한 에이전트는 관리자의 개입 없이 독립적으로 임무를 수행하도록 하여 사용자가 네트워크에 접속하고 있지 않은 경우에도 관리자를 대행하여 태스크를 수행한다. 에이전트들은 상호 독립적으로 태스크를 수행하며 사용자들이 로그아웃(log out) 할 때까지 모니터링 하여 로그 데이터를 수집한다.

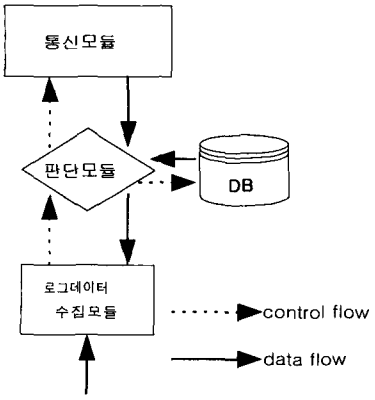

그림 2. 에이전트 모듈 내부구조

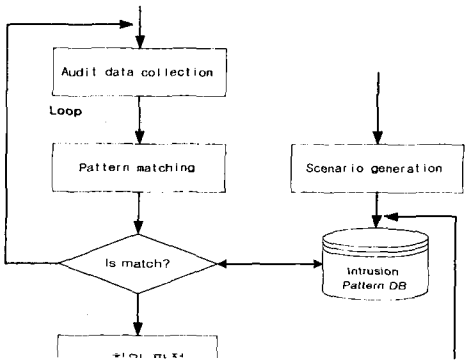

그림 3. 탐지 모듈 구성도

수집된 로그 데이터는 침입탐지 메인 호스트에 있는 학습 모듈로 전송되어 각각의 사용자들에 대한 행동 패턴을 다양한 각도에서 분류한다. 이렇게 분류된 각 사용자들의 행동 패턴은 침입 패턴 데이터베이스(Intrusion Pattern DB)에 저장한 다음 지속적으로 에이전트와 통신하면서 패턴 데이터를 교환한다. 그림 2는 에이전트 모듈의 내부 구조를 나타낸 것이다.

```
Intrusion_Detection Report()
{
 If Intrusion_Detection = intrusion then
 send signature = kill(pid);
 wtite(audit);
 warning(display);
}
```

그림4. 침입 상태 보고 알고리즘

IV. 침입 탐지 시스템

각 호스트에서 수집된 표준화된 로그 데이터는 이미 침입 탐지 시스템 데이터 베이스에 저장되어 있는 침입 패턴과의 매칭을 통해 침입을 판단한다. 이때 데이터베이스에 저장되어 있는 감사 데이터는 지속적인 학습을 통해 새로운 유형의 침입 패턴을 계속 갱신(update)한다. 또한 미리 정의해 놓은 규칙들로부터 변형된 침입 패턴을 예측·생성한다.

침입 탐지 모듈에서 침입이라고 판명되면 그림 4와 같이 침입 보고와 함께 대응 동작을 하게된다. 침입으로 판명되면 침입 탐지기에서는 해당프로세서에 바로 KILL 신호를 보내서 동작을 중지시키고 침입 탐지 서버의 DB에 해당 로그파일을 기록하고 침입자에게는 경고 메시지를 보내게 된다. 물론 침입자와의 연결이 강제로 종료되며 관리자의 콘솔을 통해 침입에 관련된 각종 정보를 확인할 수 있다.

V. 결론 및 향후 연구 방향

본 논문에서 제안된 시스템은 분산된 환경에서 기존의 에이전트 학습 방식인 기계학습 대신에 데이터마이닝 학습 모듈을 탑재하여 감사 데이터를 효율적으로 추출하였으며, 이종간에 발생하는 감사 데이터를 표준화하였다. 본 논문에서 제안한 시스템의 기대 효과를 요약하면 다음과 같다.

첫째, 에이전트 학습 방법에 기존의 기계학습 방법 대신에 데이터마이닝 학습 방법을 적용하여 각종 응용 시스템에서 발생하는 이벤트(event)들을 효율적으로 수집·분류하는데 이용할 수 있다. 특히, 시스템 보안이나 전자상거래 분야에서 분석과 예측에 필요한 데이터 수집에 용이하게 응용될 수 있다.

둘째, 감사 데이터의 수집과 분류 시 이종간에 발생하는 각종 감사 데이터들을 효율적으로 관리하기 위한 감사 데이터 표준화 방법은 분산 침입 탐지 시스템에서 널리 응용되리라 믿는다.

셋째, 끊임없이 탄생하고 있는 다양한 침입 방법을 탐지하기 위해서는 다양한 침입 패턴에 대한 예측이 필요하다. 데이터마이닝 IDS는 수집된

감사 패턴으로 다양한 패턴들을 예측할 수 있으므로 대규모의 네트워크에서의 응용이 가능하다.

향후 연구 방향으로는 본 논문에서는 감사 데이터 학습 단계를 오프라인(offline)으로 처리하여 전체적인 시스템의 부하를 최소화하였으나, 온라인(online) 상태에서 수행하여 자동화된 침입 탐지 시스템을 구축하는 연구가 필요하다. 또한 감사 데이터 학습과정에서 최소 임계값을 결정하는 문제가 크게 대두되었다. 임계값을 크게 하면 수집된 데이터들에서 정확한 감사집합을 구하지 못해 부정적 결함(False negative)이 발생할 수 있다. 따라서 감사 데이터 학습 시 적절한 임계값 설정에 대한 연구가 필요하다.

참고문헌

[1] T. Lane and C. E. Brodley. "Temporal sequence learning and data reduction dor anomaly detection". In Processsing of the fifth ACM Conference on Computer and Communications Security, pages 150-158, 1998.

[2] W. Lee, R. Nimbalkar, K. Yee, S.Patil, P. esai,T. Tran, and S. J. Stolfo. "A data mining and CIDF based approach for detecting ovel and distributed intrusions". In Proceedings of the 3rd International Workshop on Recent Advances in intrusion Detection, October 2000.

[3] W. Lee, S. J. Stolfo. "Data mining approaches for intrusion detection". In Proceeding of the 1998 USENIX security Symposium, 1998.

[4] W.Lee, S.J.Stolfo, and K.Mok, " A Data Mining Framework for Building Intrusion Detection Models", 1999 IEEE Symposium on security and Privacy, 1999.

[5] Sandeep Kumar, gene Spafford. "A Pattern Matching Model for Misuse Intrusion Detection", Proceedings of the 17th National Computer Security Conference, October 1994.