리눅스 상에서 프로세스 실행 기록을 통한 패턴 분류

Classifying Patterns through Process Execution Traces on the Linux System

김균섭 , 김금실 , 한명묵
경원대학교 전자계산학과 대학원
Kyun-Soup Kim · Jin-Shi Jin · Myung-Mook Han
Graduate of Computer Engineering, Kyungwon Univ.
E-mail : ind5124@hanmail.net

요 약

본 논문에서 리눅스 프로세스들의 패턴들(정상행위 와 비정상행위)을 학습하고 그 밖에 예비 시험들의 확장을 제시하는데 의가 있다고 할 수 있다. 패턴들은 리눅스 시스템들 안에 오용과 침입들을 확인 할 수 있도록 사용하였다. 리눅스 sendmail 프로세스의 처리의 정상행위 그리고 비정상 행위들을 위해 운영체제 호출 순차들에서 기계 학습 작업을 고안하였다. 이 방법은 테스트 기록 데이터의 정상행위로부터 sendmail의 비정상행위의 실행을 모두 정확하게 구별할 수 있는 것을 보여준다. 예비 시험들은 기계학습이 침입탐지 서비스를 제공하기 위하여 저장 된 순차 정보를 추출화 함으로써 중요한 역할을 다 할 수 있다는 것으로 나타냈다.

키워드: 리눅스 프로세스, 기계학습, 침입탐지, 데이터 마이닝

1. 서론

컴퓨터와 통신 기술의 발달로 컴퓨터 시스템과 관련된 예기치 않은 침입 및 범죄에 의한 피해가 급증하고 있는 추세이다. 네트워크 시스템들의 빠른 발전에 따른 침입들은 더 대중화가 되었다. 컴퓨터 침입들은 더 많고 다양한 커다란 피해를 결과적으로 보여주고 있다. 이러한 결과를 대처하기 위해서 효과적이고 보다 많은 노력과 빠른 검출 방법들이 제시 되어지고 있으며, 네트워크 시스템을 대표적으로 말한다면 서버 시스템을 들 수 있는데, 우리가 많이 사용하고 비용이 적게 들어가는 이점과 오픈 소스의 장점이 있는 리눅스 서버 시스템을 많이 사용하고 있는 실정이며, 이에 따른 리눅스 서버에서 침입탐지를 위한 노력이 필요할 때라고 보여 집니다. 현재에도 많이 사용되어지고 있는 sendmail의 보다 안전한 활용을 위하여 기계학습을 통한 비정상적인 침입을 탐지하는 것이 무엇 보다 중요한 시점이라고 생각하며, 많은 연구와 실험이 필요하다고 본다. 본 논문에서 이러한 점에서 큰 의를 가진다고 할 수 있다. 2장에서는 관련연구에 따른 기초설명, 3장에서는 제안하는 실험, 4장에서는 결론과 향후 과제로 맺는다.

2. 정보보호 및 데이터 마이닝

2.1 침입탐지 시스템

침입탐지란 불법적인 행위를 실시간으로 감시하여 탐지 하는 것을 말하며, 이러한 행위를 실시간으로 탐지하여 보고하는 시스템을 침입탐지 시스템이라 한다. 방화벽이 단순히 불법적인 접근을 막는데 중점을 두고 있다면 침입 탐지 시스템은 방화벽이 효과적이지 못할 때, 이에 따른 피해를 최소화하고 관리자가 없을 때에도 불법적인 침입에 적절히 대응할 수 있는 해결방안이라고 할 수 있다.[1,2,3]

2.2 침입탐지시스템 분류

침입 탐지의 2가지 기본접근 방법

2.2.1 오용 탐지(Misuse Detection)모델

오용(misuse) 침입이란 공격에 관한 축적된 지식을 사용하여 침입의 증거를 찾는 방식으로 오용탐지(misuse detection) 또는 지식기반 기법이라고 한다. 예를 들면, finger나 sendmail의 버그를 통한 인터넷 웜(Worm)의 공격 형태가 오용 침입의 대표적인 경우라고 말할 수 있다. 또한 오용탐지 기법은 기존에 잘 알려진 침입일 경우에 높은 탐지 성능을 보여 주지만 잘 알려지지 않은 침입일 경우에는 탐지할 수 없다는 단점이 있다. 오용(misuse)침입 탐지 방법의 종류로는 전문가 시스템(Production/Export System), 흔적분석(Signature Analysis), 패트리넷(Petri-net), 상태 전이 분석(State Transition Analysis)이 있습니다.[9]

2.2.2 비정상적인(anomaly) 침입 모델

비정상적인(anomaly) 침입이란 사용자행위에 관한 정상행위모델을 생성한 후 여기에서 벗어나는 경우를 찾는 방식으로 비정상 행위탐지(anomaly detection) 또는 행동기반 기법이라고 한다. 예를 들면, 한 사용자가 시스템 내에서 항상 해오던 작업 외에 관리자 영역에 들어온다던지, 시스템 내의 중요 파일을 삭제하려고 시도하는 경우 올바른 로그인 이름과 패스워드를 사용한 정당한 사용일지라도 침입으로 간주하는 경우를 들 수 있다. 비정상행위 침입 탐지 방법의 종류에는 통계적 기법(Statistical approaches), 신경망(Neural Network), 컴퓨터 면역학, 데이터 마이닝(Data Mining), HMM(Midden Markov Model)이 있습니다.[8]

2.3 데이터 마이닝(Data Mining)

데이터 마이닝(DM)은 방대한 데이터 자료로부터 숨어있는 지식이나 유용한 정보를 추출하는 과정이다. 방대한 데이터베이스로 부터 숨어있는 예측정보의 추출이라고 설명할 수도 있다. 방대한 데이터베이스에 존재하고 있는 숨겨진 관계와 전체적인 패턴을 찾는 것이다. DM은 정보나 의사결정을 식별하기 위해서 다양한 기술들을 사용하는 것으로 자료들로부터 지식(Knowledge)을 추출하여 의사결정 지원, 예측, 추정과 같은 영역에 사용될 수 있도록 한다.

그림1을 간단하게 설명하면, 먼저 선택(Selection)의 단계: 어떠한 범주에 의해서 자료를 선택하거나 분할한다. 사전처리(Preprocessing) 단계는 어떤 정보가 이동되는 자료를 정화하게 된다.

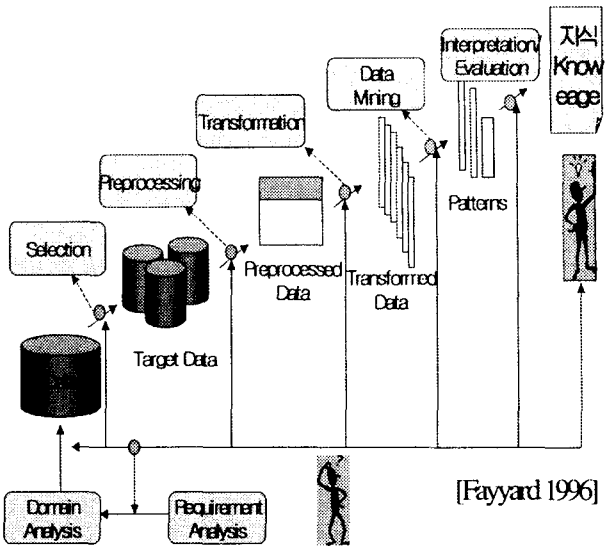

그림 1 데이터 마이닝 흐름도

변형(Transformation)은 자료가 단순하게 이동된 것이 아니라 변형이 되어서 사용되거나 탐색할 수 있게 된다. DM은 자료로부터 어떠한 패턴을 추출하는데 관심이 있는 단계이다. 여기에서 패턴이란 어떤 사실(facts)들의 집합으로 정의될 수 있다. 해석과 평가 단계: 시스템에 의해서 식별된 패턴들은 인간의 의사결정 지원에 사용될 수 있는 지식-업무의 예측과 분류 그리고 데이터베이스의 내용 요약 또는 관찰된 현상의 설명으로 해석된다.[16]

2.3.1 Classification (분류)

분류자들은 시스템 행동 측면에서 각각의 모델을 기술, 기본(base) 분류자 들이다. 다중 기본 분류자들로부터 결합된 증거는 침입탐지에서의 유효성을 향상시키는 것과 같다. 본 연구의 주안점은 다중(기본) 탐지 모델들로부터 증거를 결합하는 (귀납적 학습) 분류모델의 연구 와 실험이다.

2.3.2 Association Rules (연관 규칙)

연관규칙의 목적은 테이터베이스 테이블로부터 다양한 특징(상태)의 상호 협력적인 관계를 정의하는 것이다. 현재 흥미로운 간단한 연관규칙 알고리즘의 상업적인 적용은 고객이 빈번하게 함께 구입하는 물품들과 상점에서 물품 배치에 연관된 정보를 사용하는 것을 결정하는 것이다.

2.3.3 Frequent Episodes(빈번한 에피소드)

연관규칙 알고리즘이 가사 데이터간의 관계를 찾고 있는 동안. Frequent Episodes는 내부감사(inter-audit)레코드 패턴을 발견하는데 사용할 수 있다. Frequent Episodes는 빈번하게 발생하는 하나의 Time window-특정한 길이-이벤트들의 집합이다.

2.4 Tcpdump

Tcpdump는 주어진 조건식을 만족하는 네트워크 인터페이스를 거치는 패킷들의 헤더들을 출력해 주는 프로그램이다. 프로그램의 특성상, 네트워크 인터페이스를 아주 심도 있게 사용하기 때문에, 실행하는 사람은 반드시 네트워크 인터페이스에 대한 읽기 권 한이 있어야만 한다.(OS dependent) 위에서 말하는 읽기 권한을 가지고 있어야 하는 파일, 혹은 Tcpdump의 퍼미션 이다.

Linux : root에서 실행하거나, root로 setuid를 설정해야 함. [17]

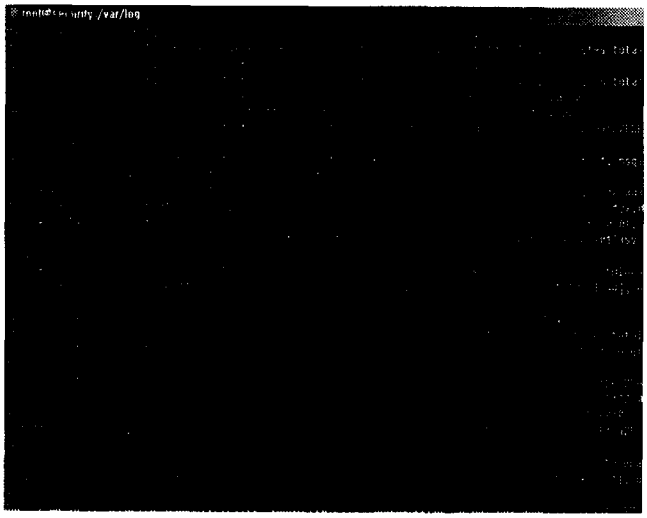

그림 2 tcpdump 캡쳐화면

2.5 침입방법

최근에 가장 많이 이용되는 침입형태를 살펴보면, 버퍼 오버플로우(buffer overflow)가 있는데, Linux 내의 프로그램을 수행하는데 명령어와 매개변수를 전달할 때, 매개변수 뒤에 다른 코드를 집어넣어 버퍼 오버플로우를 유발시킨다. 서비스 방해 공격은 네트워크를 통하여 대량의 메일을 보내거나 쓸모없는 문자를 계속 목적 호스트에 보내어 시스템의 작동을 방해하는 공격이다. 이 방법은 최근에 늘어나는 공격방법으로 방화벽(firewall)이나 패킷 필터링을 통하여 대응할 수 있다. 스니핑(sniffing)은 네트워크의 한 호스트에서 실행되어 그 주위를 지나다니는 패킷을 엿보는 방법으로 ID와 패스워드를 알아내기 위하여 침입자들에 의해 자주 사용된다. 네트워크 보안에 신경을 쓴 호스트라도 주변의 호스트가 공격당해서 스니핑을 위해 사용된다면 무력해질 수 밖에 없다. 스푸핑(spoofing)이란 자신을 타인이나 다른 시스템에서 속이는 행위를 의미한다. 예를 들어, 특정 호스트에게만 접근권한을 준다고 가정했을 경우 해커는 당연히 자신이 특정 호스트로부터 접근하려는 것처럼 속이려 할 것이며, 이를 가로채 바로 스푸핑이라고 할 수 있는 것이다.

3. 지식기반 침입탐지 정보화 모델

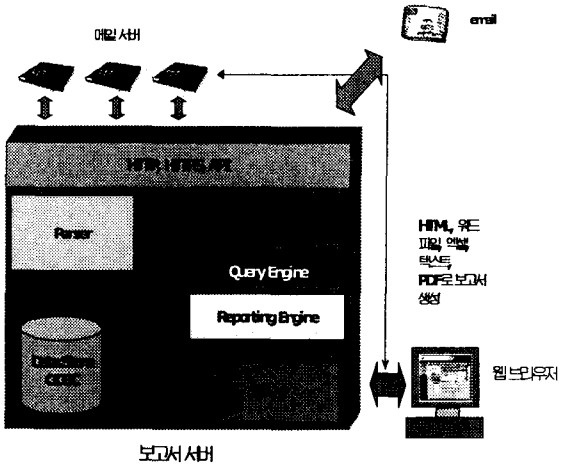

그림 3 sendmail 분석기 구조

그림 3에 나온 모델을 통해서 얻어지는 정보로는 인터넷에서 메일 송수신한 트래픽에 관한 정보 최고/최소 송수신 도메인(메시지 수, 메시지 크기), 일일 평균 메시지 트래픽, 시간에 따른 일일 최대/최소 메시지 트래픽, 주간별 일일 메시지, 주중 최고 트래픽 요일, 최고 트래픽 시간, 시간당 메시지 수, 시간당 배달 소요시간, 사이트/서버별 배달 소요시간, 키워드를 가진 송수신 메시지등이 있다. Rules/Filters에서 규칙을 생성해서 출력을 가시화 하고 판단하는 묘듈을 추출하게 된다. 외부 또는 내부에서 발생하는 자료(패킷)를 ethereal이라는 GUI 인터페이스를 통해서 패킷을 캡쳐 하는데 여기서 사용 레이어로 사용 되어지는 Wincap은 Win32환경에서 패킷을 캡쳐하고 네트워크를 진단할 수 있는 라이브러리이다. Unix/Linux의 libcap라이브러리와 유사한 기능을 제공한다.[7][14][15]

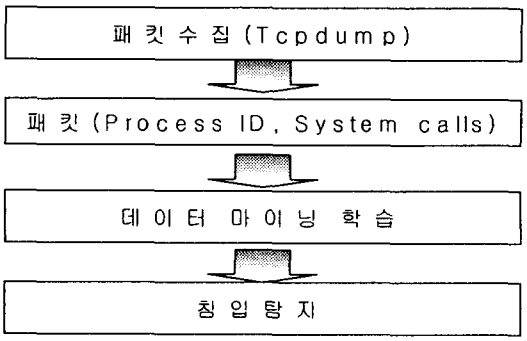

그림 4 제안된 침입탐지시스템 흐름도

본 실험에서 제시하는 데이터 마이닝을 이용한 침

입탐지 시스템의 흐름도는 그림 4와 같다.
① 패킷 수집기는 Tcpdump를 이용하여 패킷을 모니터링하고 ethereal로 데이터 정보를 파일로 캡처한다. ② 패킷을 Process ID, System calls로 dump된 16진수값에서 역으로 추출해야하는 작업을 통해서 수치화 한다. ③ 데이터 마이닝 학습을 시켜서 '정상', '비정상'인지 레이블로 구분하고 오류율이 최소화 시킨다.④ 침입을 탐지해 낸다. 마지막 부분이 가장 중요한 단계라고 할 수 있는데 기존에 로그분석기에서는 패킷을 분석하고 그에 따른 조치나 실시간 상황파악이 안 돼는 경우가 많았으며, 오류율이 높은 단점을 지니고 있었으나, 본 논문에서 제안하는 분석모델은 지능적으로 해석하고, "비정상행위"를 하는 사용자를 판단하거나 차단하는 기능, 시각적으로 가시화하는 부분에서 단점을 보완하였다고 볼 수 있다. 대중성이 있고, 편리하게 자료(방대한 양의 패킷)를 구분하여 정보화 할 수 있는 모델이 제시 되었다는데 주안점을 들 수 있다.[10]

4. 결론 및 향후과제

리눅스 운영체제는 공개 S/W중에 가격이 저렴하여 비용이 적게드는 장점을 가지고 있다. 그 중 리눅스 운영체제는 인터넷 서버로서 그 활용이 광범위하며 보급률이 날로 증가추세이다. 이에 반해서 다양해져가는 해킹기법 및 불법적 사용시도에는 매우 약한 결점을 가지고 있는 것도 사실이다. 이러한 현상에서 기존의 방화벽이나 IDS같은 보안제품이나 응용 프로그램으로 보안성을 확보하기에는 한계가 있다. 이에 본 논문에서는 해킹방지와 요구사항을 중심으로 리눅스 sendmail 프로세스의 처리의 정상행위 그리고 비정상 행위들을 위해 운영체제 호출 순차들에서 데이터 마이닝을 통한 기계 학습 작업을 고안하였다. 다소 적은 영역을 나타내고 있지만 리눅스 운영체제의 보안과 성능향상에 향후 공개 소프트웨어의 기술력과 해킹방지(예방차원)에 대한 계속적인 연구가 필요하고, 공개S/W의 발전과 국가 정보화 사회에 따른 국가경쟁력을 높이는 차원에서 많은 관심이 필요할 때 이다.

5. 참고문헌

[1] 한국정보보호센터, "정보통신시스템 침해사고방지 기술 개발", 1999. 1.
[2] 한국정보보호센터, "'98 해킹 및 대응 현황", 1998. 12.
[3] 한국정보보호센터, "'98 CERTCC-KR 연보", 1999. 3.
[4] H. T.Jung. et. al., "Caller Identification System in the Internet Environment," Proceedings of the USENIX Security Symposium IV. 1993.
[5] Philip K. Chan and Salvatore J. Stolfo. 1993. Toward Parallel and Distributed Learning by Meta-Learning. In working Notes of AAAI Work. Knowledge discovery in Databases, 227-240
[6] Stephanie Forrest, Steven A. Hofmeyr, Anil Somayaji, and Thomas A. Longstaff 1996. A Sense of Self for Unix Processes. in Proceedings of the 1996 IEEE Shymposium on Security and Privacy, 120-128. IEEE Computer Society Press, Los Alamitos, CA.
[7] SSL/TLS를 이용한 Management Agent(M/A) 구조상의 Network IDS 설계 및 구현
[8] H. Javitz et al., "Next generation intrusion detection expert system (NIDES) - 1. statistical 미해갸소 ㅡㄴ rationale -2. rationale for porposed resolver," Technical Report A016-Rationales, SRI International, March 1993.
[9] B. Mukherjee, T. L. Heberlein and K. N. Kevitt, "Network intrusion Detection,"IEEE Network, Vol8, No.3, pp.26-41, May/June, 1994.
[10] UNIX 환경에서 퍼지 Petri-net을 이용한 호스트 기반 침입 탐지 모듈 설계
[11] http://trade.chonbuk.ac.kr/~leesl/mail
[12]http://www.superuser.co.kr/sendmail/sendmail_relay_test/index.htm
[13]http://www.cs.umn.edu/research/minds/intrusion_detection.htm
[14]http://winpcap.polito.it/
[15]http://www.ethereal.com/
[16]http://www.cs.umn.edu/research/minds/intrusion_detection.htm
[17]http://security.kaist.ac.kr/docs/tcpdump.html