2002년 한국정보처리학회 춘계학술발표논문집 제9권 제1호

시스템 호출을 이용한 침입예상 데이터베이스 기반 침입탐지

고기웅* 신욱 이동익
광주과학기술원 정보통신공학과
{fishbear*, sunihill, dilee}@kjist.ac.kr

Intrusion Detection based on Intrusion Prediction DB using System Call Sequences

Ki Woong Ko*, Wook Shin and Dong-Ik Lee
Dept of Information and Communications,
Kwangju Institute of Science and Technology

요 약

본 논문에서는 중요 프로세스(privileged process)의 시스템 호출 순서(system call sequence)를 이용한 침입탐지 시스템을 제안한다. 기존 연구의 정상행위 기반 침입탐지 시스템은 정상행위를 모델링하여 시스템을 구성하고, 이와 비교를 통해 프로세스의 이상(anomaly) 여부를 결정한다. 이러한 방법은 모델링되지 않은 미지의 행위에 대한 적절한 판단을 행할 수 없으므로, 높은 오류율(false-positive/negative)을 보인다. 본 논문에서는 현재까지 알려진 공격에서 공통적으로 나타나는 윈도우들을 수집하여 침입예상윈도우를 구축하고, 이를 기존의 침입탐지 시스템에 부가적으로 사용하여 효과적으로 오류율(false-positive/negative)을 낮출 수 있음을 보인다. 실험 결과 제안된 방법을 통한 침입탐지는 기존의 방법에 비해 공격 탐지율은 증가하고 정상행위에 대한 오류율은 감소하였다.

1. 서 론

침입탐지(intrusion detection)란 외부에서 시도되는 시스템 침투나 내부의 권리 남용과 같은 전체적인 보안 이상을 탐지하는 것으로 컴퓨터 보안 시스템의 중요한 부분을 담당하고 있다[1]. 침입탐지시스템은 사용자(user) 혹은 중요 프로세스(privileged process)의 행위(behavior)를 모델링하여 데이터베이스를 구축하고, 이를 판별하고자하는 대상의 행위(behavior)와 비교하여 침입을 판별한다. 이중 정상행위를 이용하여 데이터베이스를 구축하는 것을 이상탐지(anomaly detection)라 하며, 비정상행위를 이용하여 데이터베이스를 구축하는 것을 오용탐지(misuse detection)라 한다.

이상탐지는 모델링되지 않은 행위는 모두 시스템에 대한 공격으로 간주한다. 그러므로 공격을 정상행위로 간주(false-negative)하는 오류는 적으나, 정상행위를 침입으로 판정하는 오류(false-positive)가 높다.

오용탐지는 기존에 밝혀진 잘 정의된 공격과 유사도 비교를 통해 침입여부를 판별하기 때문에, 정상행위를 공격으로 간주하는 오류(false-positive)가 적다. 하지만 정의되지 않은 공격은 탐지하기 어려워, 공격을 정상행위로 간주하는 오류(false-negative)가 많다.

이상/오용탐지는 각각에 대해서 침입 판별을 위한 비교 기준을 필요로 한다. 이러한 비교 기준으로는 시스템의 작업 기록인 감사(audit)서비스를 통해 수집된 공격 패턴이나 정상행위 패턴 정보가 많이 사용된다. 이렇게 수집된 정보는 기계 학습(machine learning)등을 통해 모델링된 후, 데이터베이스로 저장되어 침입판별을 위한 기준으로 사용된다.

모델링 방법은 그 대상에 따라 사용자(user)의 행위를 모델링[1][3][4]하는 방법과 중요 프로세스(priviliged process)를 모델링하는 방법[2]으로 나눌 수 있으며, 적용 방법에 따라 윈도우 기반 순서나열법, 확률적 접근 방법, 상태전이그래프를 이용한 방법으로 나눌 수 있다[5]. [5]에 의하면 현재까지의 모델링 방법들 중 윈도우 기반 순서나열법의 성능이 제일 우수한 것으로 알려져 있다.

본 논문에서는 솔라리스(SUN Solaris)의 감사 모듈(Audit Module)인 BSM(Basic Security Module)으로부터 얻을 수 있는 프로세스의 시스템 호출 순서(system call sequence) 정보를 행위 모델링에 사용한다. 모델링의 대상은 sendmail, ftp, lpr등 모든

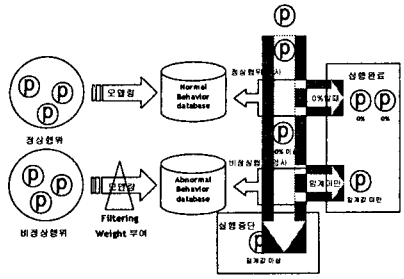


그림 1. 침입탐지 아키텍처

프로세스가 가능하나, 본 논문에서는 그 중 가장 빈번하게 쓰이며 공격에 많이 이용되는 프로세스인 sendmail을 대상으로 하였다. 또한 행위 모델링을 위해 윈도우 기반 순서 나열법을 사용하며, 미지의 정상행위와 알려지지 않은 공격을 효율적으로 탐지하기 위한 침입 예상 데이터베이스를 도입한다. 기존 방법에 침입 예상 데이터베이스를 부가적으로 사용함으로서 오류율(false-positive/negative)을 감소시키고, 공격의 탐지율을 향상시킬 수 있다.

2장에서는 정상행위 모델링에 관련하여 윈도우 기반 순서 나열법에 대해 설명하고, 그에 따른 문제점을 지적하며, 3장에서는 본 논문에서 제시하는 침입 예상 데이터 베이스의 생성방법 및 적용방법에 대해서 설명한다. 4장에서는 침입 예상 데이터베이스 도입에 따른 성능개선의 효과를 보이는 실험결과를 제시한다. 마지막으로 5장에서 결론과 향후연구 방향에 대하여 다룬다.

2. 관련 연구

시스템 콜을 이용한 이상 침입탐지 시스템 연구의 효시는 뉴멕시코 대학(University of New Maxico)의 Forrest의 연구가 최초이다[6]. [6]에서는 윈도우 크기 k를 정의한 다음, 각각의 시스템 콜에 대하여 k개의 lookahead를 구성하여 데이터베이스를 구축한다. [7]은 기존의 방법을 침입 탐지율 측면에서 개선된 접근법으로 기본적인 아이디어는 동일하나 시스템 콜 순서를 k개 단위 크기로 잘라 데이터베이스를 구성한다. [8]은 각각의 시스템 콜에 따른 적절한 윈도우 사이즈를 찾고 이를 정상행위 데이터베이스의 구성에 반영함으로서 기존의 방법[6][7]보다 좋은 성능을 보인다. [9]는 시스템 콜을 통해 유한상태기계를 학습하여 정상행위 데이터베이스를 구축한다. 기존의 방법보다 학습 속도가 빠르고 오류율도 낮으나, 유한상태기계를 구성하기 위한 제약조건이 많아 현실적으로 적용이 어렵다.

기존 연구인 [6][7][8][9]는 정상행위만을 고려하여 DB를 구성하였다. 그러나, 이러한 방식은 상대적으로 비정상행위에 대한 정보가 부족하므로, 모델링되지 않은 미지의 행위에 대한 침입여부 판단을 적절히 행할 수 없다. 비정상 행위를 고려하기 위해 이상탐지와 오용탐지를 중복시켜 사용하는 것도 한 해결책이 될 수 있으나, 시스템 콜을 통해 나타나는 모든 침입들은 정상행위와의 유사도가 90%이상이므로 패턴의 중복으로 인한 오버헤드가 크고, 침입에 해당하는 부분만을 별도로 정의하기가 어렵다[6][7]. 또한 오용탐지를 중복 사용한다고 하더라도 그 특성상 발견되지 않은 침입은 탐지하기 힘들다. 이에, 본 연구에서는 정상행위 DB를 기반으로 하되, 침입 예상 데이터베이스라는 별도의 정보를 부가적으로 활용함으로써 위의 문제를 해결하고자 한다.

3. 침입 탐지 아키텍처

본 논문에서 제안하는 침입탐지 아키텍처는 그림 1 과 같다. 제안된 침입탐지 아키텍처는 크게 **정상행위 검사와 비정상행위가능성검사**로 나뉜다. 정상행위 검사는 정상행위 데이터베이스와 비교를 통해 이루어지며, 비정상행위가능성 검사는 3.1에서 설명할 침입 예상 데이터베이스를 통해 이루어진다. 제안된 침입탐지 시스템은 검사할 프로세스의 시스템 콜의 호출 순서를 실시간으로 정상행위 데이터베이스와 비교하여, 정상행위를 벗어나지 않으면 프로세스의 실행을 완료한다. 하지만 비교 도중 조금이라도 정상행위를 벗어나면, 그 순간부터 침입예상데이터베이스를 통해 벗어난 부분을 비교한다.

데이터베이스를 생성하는 방법과 이를 통해 침입을 탐지하는 방법은 다음과 같다.

3.1 정상행위 데이터베이스의 생성

본 논문에서는 정상행위데이터베이스 구성은 기본적으로 [7]의 방법으로 모델링하며 아래와 같이 정규표현(regular expression)으로 재정의 한다.

정의 1.(윈도우) 스트링 w는 길이가 k인 어떤 문자열 s의 부분문자열(substring)이며 윈도우로 정의.

Σ : 시스템 콜의 알파벳. 단 시스템 콜은 각각은 하나의 기호에 대응함

부분문자열(substring): $x, y, z \in \Sigma^*$ 이고 $w = xyz$ 이면, y는 w의 부분문자열이다. $y \sqsubset w$로 나타낸다.

s : (시스템 콜 순서), $s \in \Sigma^+$

정의 2. (정상행위 데이터베이스) 알파벳 Σ 와 $s_n \in \Sigma^+$ 인 정상행위 시스템 콜 순서 s_n 에 대해 정상행위 데이터베이스는 집합 D_N로 나타내며

$$D_N = \{\, w \mid {}^{\forall} w \sqsubset s_n \,\}$$

로 정의한다.

3.2 침입 예상 데이터베이스의 생성

이번 절에서는 침입 예상 데이터베이스를 생성하는 방법에 대해 설명한다. 침입 예상 데이터베이스는 현재까지 밝혀진 공격에 나타나는 윈도우들 중 정상행위가 아닌 것들을 추출하여 생성된다. 각각의 공격에 대해 나타나는 윈도우들은 그 특성상 중요프로세스의 동일한 약점을 공격하기 때문에, 비슷한 시스템 콜을 호출하게 되며, 비슷한 형태의 윈도우를 생성한다. 즉 아직 발견되지 않은 공격도 중요프로세스의 동일한 약점을 공격할 것이며, 기존의 공

표 1. 공격사이에 공통으로 존재하는 윈도우의 개수

Win#:7	Attack1	Attack2	Attack3	Attack4	Attack5	Attack6	Attack7	Attack8	Attack9
Attack1	353								
Attack2	205	295							
Attack3	191	181	259						
Attack4	216	224	167	244					
Attack5	6	5	6	4	130				
Attack6	16	16	16	16	4	70			
Attack7	16	17	16	17	4	31	44		
Attack8	34	34	34	34	4	12	12	88	
Attack9	99	105	99	93	16	16	17	34	537

격과 비슷한 형태의 윈도우를 생성할 것이다. 그러므로 기존의 발견된 공격을 통해 밝혀지지 않은 공격도 효과적으로 탐지할 수 있다. 각 공격들이 공통적으로 갖는 윈도우의 개수를 측정한 결과 표 1을 얻을 수 있었다. 표 1은 윈도우의 사이즈가 6일 때 각각의 유형이 다른 공격에서 정상 윈도우를 제외하고 공통적으로 갖는 윈도우들의 수이다.

침입 예상 데이터베이스는 현재까지 밝혀진 공격에서 정상행위를 제한 부분을 윈도우로 만들어 저장한다. 비정상 윈도우는 다음과 같이 정의한다.

정의 3. (침입 예상 데이터베이스) 비정상행위 시스템 콜 순서(abnormal system call sequence) $s_{ab_0}, s_{ab_1}, \ldots, s_{ab_n}(0 \le n)$에 대해 다중집합(multi-set) $D_{S_{ab_i}}$

$$D_{S_{ab_i}} = \{\ w \mid {}^{\forall} w \sqsubseteq s_{ab} \wedge w \notin D_N \ \} \quad (0 \le i \le n)$$

로 정의하며, 침입 예상 데이터베이스는 다음과 같이 다중집합 D_{ab}

$$D_{ab} = D_{S_{ab_0}} \cup D_{S_{ab_1}} \cup \ldots \cup D_{S_{ab_i}}$$

로 정의한다.

3.3 예 제

본 절에서는 정상행위 데이터베이스와 침입 예상 데이터베이스의 생성에 대해 이해를 돕기 위한 예제를 제시한다.

알파벳 $\Sigma = \{open,\ read,\ mmap,\ getrlimit,\ close\}$에서 정상행위 시스템 콜 순서 s_n와 비정상행위 시스템 콜 순서 s_{ab} 가 다음과 같을 때

s_n = *open read mmap mmap open getrlimit mmap close*

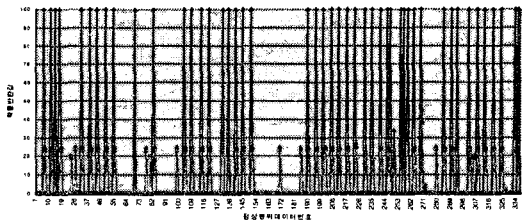
s_{ab} = *open read open mmap open getrlimit mmap close*

윈도우의 크기가 4($k=4$)인 정상행위데이터베이스 및 침입예상데이터베이스는 다음과 같이 구성된다.

D_N={*open read mmap mmap, read mmap mmap open, mmap mmap open getrlimit, mmap open getrlimit mmap, open getrlimit mmap close* }

$D_{S_{ab}}$={*open read open mmap, read open mmap open, open mmap open getrlimit* }

그림 2. false-positive측정을 위한 확률반환값의 비교



3.4 침입 탐지법

침입탐지시스템은 프로세스의 검사결과로 이상행위 가능성을 확률값으로 반환한다. 반환된 확률값은 보안관리자에 의해 정해진 임계값과 비교되어, 임계값 이상일 경우 침입으로 판단된다. 기존의 연구에서는 정상행위 데이터베이스만을 고려하지만, 본 논문에서는 침입 예상 데이터베이스를 추가로 사용했기 때문에 이를 고려할 수 있는 확률 반환값이 필요하다. 본 논문에서는 반환하는 확률값을 다음과 같은 공식을 기반으로 계산한다. 검사하고자 하는 프로세스 P에 대해

$$\text{확률반환값: } R_s = \frac{\alpha \cdot N_{miss} + (1-\alpha) \cdot A_{match}}{\alpha \cdot |P_w| + (1-\alpha) \cdot A_{match}} \times 100\ (\%)$$

α : 정상 행위 모델링에 대한 신뢰도 (상수)
$|P_w|$: 프로세스 P를 통해 만들 수 있는 윈도우의 갯수
N_{miss} : P를 윈도우로 만든 후 D_N에 존재않는 윈도우의 갯수
A_{match} : P 를 윈도우로 만든 후 D_{ab}에 존재하는 윈도우의 개수

위의 식에서 α는 정상행위 정도에 대한 신뢰도이며 침입탐지 시스템을 쓰는 사용자가 지정하는 상수로 0에서 1까지 변할 수 있다. α는 일종의 가중치로서 조사하는 프로세스에 대해서 정상행위 데이터베이스와 침입 예상 데이터베이스의 값을 어떤 비율로 참고하여 확률반환값을 만들 것인가에 대한 기준이다. 예를 들어 α가 0.5라면 정상행위 데이터베이스와 침입 예상 데이터베이스를 각각 반반씩 참고하여 확률반환식을 계산한다. 그러므로 α 사용하여 정상행위 모델링 정도나 침입 예상 모델링 정도에 따라 시스템을 잘 조율할 수 있다.

4. 실험 결과

실험을 위한 데이터[9]는 뉴멕시코대학에서 제공하는 정상행위의 시스템 콜 순서와 공격의 시스템 콜 순서를 사용하였다.

4.1 정상행위에 관한 실험

본 실험에서는 모델링되지 않은 정상행위를 얻기 위해서, 정상행위 데이터베이스의 크기를 제한한다. 즉 뉴멕시코대학에서 제공하는 336개의 정상행위 시스템 콜 순서 중 정상행위데이터베이스를 생성하는데 일부만 이용하면 나머지는 시스템 콜 순서는 데

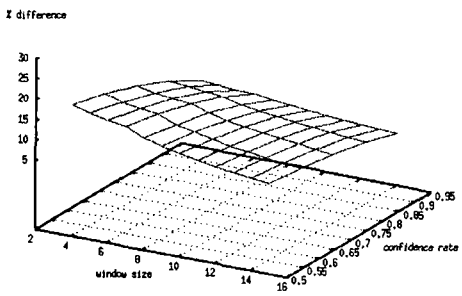


그림 3. 공격탐지율의 증가

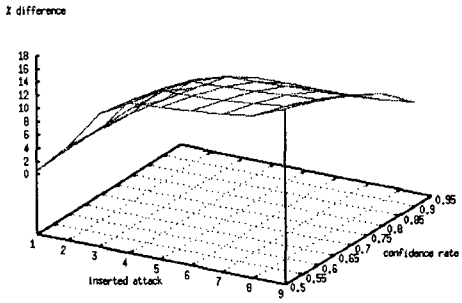


그림 4. 공격추가에 따른 탐지율의 증가

이터베이스에 포함되지 않기 때문에 이를 통해 false-positive를 만들 수 있다. 정상행위 데이터베이스에 생성에 사용한 정상행위는 10%부터 100%까지 변화시키며 측정했고, α 는 0.5에서 1.0 , 윈도우 크기 4에서 15까지 실험하였다. 본 논문에서는 지면관계상 그 중 일부만 제시한다. 모든 실험결과에 대한 그래프는 [8]에 기술되어 있다.

그림 2는 α =0.8이고 윈도우 크기는 7 일때, 기존 데이터의 78%을 이용해 정상행위데이터베이스를 구축했을 때 얻은 결과이다. x축은 정상행위번호이며 y축은 반환확률값이다. 세모꼴은 기존연구에서 탐지한 반환확률값이며 네모꼴은 본 논문에서 제안한 방법을 통해 계산했을 때 얻는 반환 확률값이다. 본 실험에서 사용한 데이터는 모두 정상행위이므로 낮은 확률값을 반환할수록 성능이 우수하다. 그림 2의 결과에서 알 수 있듯이 제안된 방법이 전체적으로 훨씬 낮은 값을 반환하므로 성능이 더 우수하여 정상행위를 더 잘 구별한다는 것을 알 수 있다.

4.2 오류 탐지율

오류탐지율은 기존에 밝혀진 9개의 공격을 사용하여 침입 예상 데이터베이스를 구성한 다음 측정하였다. 그림 3은 각 윈도우 사이즈와 α값에 따라 평균적으로 기존의 공격을 얼마만큼 더 높은 확률로 탐지했는가를 보여주는 그래프이다. 각각의 공격 탐지율은 기존의 방법에 비해 모두 증가하였으며, 평균적으로 20% 더 높은 확률로 탐지를 하고 있음을 볼 수 있다. 그림 4는 공격추가에 따른 탐지율의 증가를 보여주는 그림으로 침입 예상 데이터베이스의 도입으로 인해 발견되지 않은 공격도 효과적으로 탐지될 수 있음을 보여주는 그래프이다. 즉 공격을 하나씩 차례대로 추가해가면서 탐지율를 보았을 때 추가되지 않은 공격도 탐지율이 높아진다는 것을 보여주는 그래프이다. 그러므로 침입 예상 데이터베이스를 이용하면 발견되지 않은 공격도 기존의 방법보다 높은 확률로 찾아낼 수 있다. 공격 각각에 따른 자세한 그래프 및 설명은 지면관계상 [8]을 참조한다.

5. 결론 및 향후연구

제안된 침입 탐지 방법은 기존의 방법보다 공격 탐지율 및 오류율에서 좋은 성능을 보인다. 즉 정상행위를 공격으로 판단할 확률과 공격을 정상행위로 판단할 확률이 기존의 방법에 비해 낮다. 또한 중요 프로세스의 특성상 비슷한 공격방법으로 인해 발생하는 공통적인 윈도우들의 성질을 이용하여 아직 밝혀지지 않은 공격을 탐지할 수 있다. 뿐만 아니라 공격의 중복을 제거함으로서 데이터베이스의 크기를 줄여 실시간 응용에 적합하다.

위 침입탐지 시스템은 향후 모듈화 하여 리눅스 커널에 탑재할 예정이며 이와 관련하여 실시간성을 더욱 개선시키기 위한 연구가 필요하다.

6. 참고 문헌

[1] D. E. Denning, "An Intrusion Detection Model," IEEE trans. on software engineering, 1989

[2] C. Ko, G. Fink, K. Levitt, "Automated Detection of Vulnerabilities in Privileged Programs by Execution Monitoring," Computer Security Applications Conference, 1994.

[3] S. E. Smaha. Haystack, "An Intrusion Detection System," Proceedings of the 4th Computer Security Application Conference, 1988.

[4] H.S. Vaccaro , G.E. Liepins, "Detection of Anomalous Computer Session Activity," Proceedings of the 1989 IEEE Symposium on Research in Security and Privacy.

[5] C. Warrender, S. Forrest, B. pearlmutter, "Detecting Intrusions Using System Calls: Alternative Data Models," IEEE Symposium on Security and Privacy, 1999.

[6] S. Forrest, S A. HofMeyr, T.A.Longstaff, "A Sense of Self for Unix Processes," IEEE Symposium on Security and Privacy, 1999

[7] S. A. Hofmeyr, S. Forrest, A. Somayaji, "Intrusion Detection using Sequences of System Calls," the Journal of Computer Security, 1998.

[8] K.W. Ko, "Intrusion Detection System," Technical paper KJIST-CSRL-TR-2001-02-25, http://csrl.kjist.ac.kr/~kwko/research/ids.html, 2002.

[9] http://www.cs.unm.edu/~immsec/data-sets.htm