시간 기반의 비정상 행위 침입탐지 모델 설계

신미예* · 정윤수** · 이상호***

A Design of Time-based Anomaly Intrusion Detection Model

Mi-Yea Shin* · Yoon-Su jeong** · Sang-Ho Lee***

요 약

시스템 호출 순서에 대한 관계를 분석하는 방법은 정상적인 시스템 호출 순서를 일정한 크기로 시스템 호출 순서를 분할하여 진을 생성하여 탐지자로 사용한다. 시스템 호출의 매개변수를 고려하는 방법은 매개변수의 길이에 대한 평균과 표준편차를 이용하여 탐지자로 사용한다. 시스템 호출 순서만을 고려한 모델은 시스템 호출 순서는 정상이지만 포맷 스트링 공격과 같이 매개변수의 값만 변하는 공격을 탐지할 수 없으며, 시스템 호출 매개변수만을 고려한 모델은 매개변수 각각을 고려하므로 공격이 시작되지 않은 구간에서 획득한 정보에 의해 긍정적 결함률이 높게 나타나는 문제점이 있다. 이러한 문제점을 해결하기 위해 공격과 관련된 시스템 호출의 여러 속성들을 동시에 고려하는 접근 방법으로서 연속적인 시스템 호출 순서 및 매개변수를 그룹(Group)화하여 보다 효율적으로 학습 및 탐지하는 방법이 필요하다. 이 논문에서는 비정상적인 행위를 정상적인 행위로 판단하는 긍정적 결함률을 개선하기 위하여 시스템 호출 순서 및 매개변수에 시간 개념을 적용하여 시스템 호출 순서 및 매개변수의 비정상행위를 탐지한다. 실험 결과 제안 기법은 DARPA 데이터 셋을 사용한 실험에서 시스템 호출의 긍정적 결함률은 시간을 고려하지 않은 시스템 호출 순서 모델보다 시간을 고려한 시스템 호출 순서 모델의 긍정적 결함률이 13% 향상되었다.

ABSTRACT

In the method to analyze the relationship in the system call orders, the normal system call orders are divided into a certain size of system call orders to generates gene and use them as the detectors. In the method to consider the system call parameters, the mean and standard deviation of the parameter lengths are used as the detectors. The attack of which system call order is normal but the parameter values are changed, such as the format string attack, cannot be detected by the method that considers only the system call orders, whereas the model that considers only the system call parameters has the drawback of high positive defect rate because of the information obtained from the interval where the attack has not been initiated, since the parameters are considered individually. To solve these problems, it is necessary to develop a more efficient learning and detecting method that groups the continuous system call orders and parameters as the approach that considers various characteristics of system call related to attacking simultaneously. In this article, we detected the anomaly of the system call orders and parameters by applying the temporal concept to the system call orders and parameters in order to improve the rate of positive defect, that is, the misjudgment of anomaly as normality. The result of the experiment where the DARPA data set was employed showed that the proposed method improved the positive defect rate by 13% in the system call order model where time was considered in comparison with that of the model where time was not considered.

키워드

호스트기반 침입탐지, 시스템 호출 순서, 시스템 호출 매개변수, 긍정적 결함, 부정적 결함

Key word

Host based IDS, System call sequence, System call argument, false-positive, false-negative

* 정회원 : 충북대학교(shinmiyea@nate.com)
** 준회원 : 한남대학교 산업기술연구소 전임연구원
*** 준회원 : 충북대학교 소프트웨어학과 교수

접수일자 : 2011. 02. 02
심사완료일자 : 2011. 05. 04

Ⅰ. 서 론

시스템 호출을 기반으로 하는 침입 탐지 방법은 시스템 호출 순서에 대한 상관관계를 분석하는 방법[1, 2, 3, 4, 5]과 시스템 호출 매개변수를 고려하는 방법[6, 7, 8]이 있다. 시스템 호출 순서에 대한 상관관계를 분석하는 방법은 정상적인 시스템 호출 순서를 일정한 크기의 시스템 호출 순서로 진을 생성하여 탐지자로 사용하고, 시스템 호출 매개변수를 고려하는 방법은 매개변수의 길이에 대한 평균과 표준편차를 이용하여 탐지자로 사용한다. 시스템 호출 순서만을 고려한 모델은 정상이지만 포맷 스트링 공격[9]과 같이 매개변수의 값만 변하는 공격을 탐지할 수 없으며, 시스템 호출 매개변수만을 고려한 모델은 매개변수 각각을 고려하므로 공격이 시작되지 않은 구간에서 획득한 정보에 의해 긍정적 결함률이 높게 나타나는 문제점이 있다. 특히, 침입탐지 시스템 중에서 시스템 호출 순서와 시스템 호출 매개변수를 이용한 모델은 긍정적 결함률이 높으며 비정상적인 시스템 호출을 정상적인 시스템 호출로 판단하여 경보(alarm)를 발생시키지 않는 문제점이 있다.

이러한 문제점을 해결하기 위해 공격과 관련된 시스템 호출의 여러 속성들을 동시에 고려하는 접근 방법으로서 연속적인 시스템 호출 순서 및 매개변수에 단위 시간 개념을 적용하여 그룹(Group)화 함으로서 비정상적인 행위를 정상적인 행위로 판단하는 긍정적 결함률을 개선한다.

이 논문의 구성은 다음과 같다. 2장에서는 시스템 호출 순서를 고려한 탐지 방법과 시스템 호출 번호 매개변수를 이용한 탐지 방법을 기술하고 3장에서는 단위 시간을 중심으로 시스템 호출 순서와 매개변수 길이에 대하여 통계적 특성을 고려한 비정상행위 침입탐지 모델을 제안한다. 4장에서는 제안 모델을 단위 시간을 고려한 긍정적 결함률과 부정적 결함률을 비교 분석한다. 마지막으로 5장에서는 결론 및 향후과제에 대한 방향을 제시한다.

Ⅱ. 관련연구

비정상 침입 탐지를 위해 시스템 호출의 특이성을 찾아내어 비정상 유무를 판단하는 시스템 호출 관련 정보를 이용한 모델에 대하여 기술한다.

2.1. 네거티브 선택(negative selection)을 이용한 모델

1994년 멕시코 대학의 S. Forrest 교수는 흉선에서 항체 T-cell이 생성될 때 몸 안에 있는 항체와 같은 T-cell은 선택하지 않는 네거티브 선택을 적용하여 컴퓨터에서 비정상적으로 실행되는 것을 탐지하기 위한 항체 생성 알고리즘을 제안하였다. 이 알고리즘은 change detection 알고리즘으로 정상적인 이진수 집합 x와 임의로 생성된 이진수 집합 y사이의 match(x,y)는 적어도 r개의 이진수가 연속해서 일치되는지를 판단한다. 면역 시스템을 이용하는 방법은 시스템 호출 순서의 길이가 짧을 때 적합한 방법이며, 인간의 신체에서 흉선으로부터 항체 T-cell을 생성하는 메커니즘을 적용한 것이 특징적이다[10, 11, 12].

2.2. 시스템 호출 순서를 이용한 모델

시스템 호출 순서는 모든 정상적인 행위의 시스템 호출에 대하여 고정된 윈도우 크기에 맞추어 시스템 호출 순서를 분할하여 탐지자로 사용한다. 시스템에서 처리되는 시스템 호출 순서와 탐지자간 불일치 정도로 공격 여부를 판단한다[13, 14, 15, 16].

2.3. 시스템 호출 매개변수를 이용한 모델

format string 공격, security critical data공격, race condition 공격 같은 침입은 비정상적인 행위에서 시스템 호출 순서에는 변화가 없으므로 시스템 호출 순서로 비정상 유・무를 판단하기가 어려우므로 시스템 호출 매개변수의 분포 및 순서 등을 이용하여 침입을 탐지하는 방법이 제안되었다[9,17].

시스템 호출 매개변수를 이용하는 방법은 프로세스가 실행되면 생성되는 시스템 호출이 실패할 경우 실패한 정보가 저장되어 있는 로그 파일을 이용하여 침입하는 것으로서 시스템 호출 매개변수에 대한 평균 μ와 표준편차 σ을 갖는 문자열 길이 분포가 예측되어질 때, 시스템 호출 매개변수 모두에 대하여 길이 l을 갖는 매개변수 문자열의 평가는 (식 1)과 같이 변수 x와 평균과의 차이가 임계값 t보다 클 가능성은 분산보다 작고 문자열 길이 l이 평균 μ보다 클 가능성 $p(l)$에 의해 판단된다.

$$p(l : l > \mu) = p(|x-\mu|) > |l-\mu|) < \frac{\sigma^2}{(l-\mu)^2} \quad \text{(식 1)}$$

Ⅲ. 시간 기반의 비정상 행위 침입 탐지 모델

단위 시간을 이용하여 시스템 호출 순서(System Call Sequence, SCS)의 유사성과 시스템 호출 매개변수(System Call Parameter, SCP)의 통계적 분포를 고려한 시간 기반의 비정상 행위 침입 탐지 모델을 기술한다.

3.1. 개요

제안 모델은 시스템 호출 순서의 연관성 분석과 매개변수의 길이에 대하여 단위 시간 개념을 적용한 침입 탐지 방법을 제안한다. 제안 모델은 시스템 호출 감사 자료에서 프로세스 ID, 시스템 호출 번호, 시간, 매개변수를 추출하여 비정상적인 시스템 호출 유・무를 판단한다. 제안 모델에서 단위시간이라 함은 정상적인 시스템 호출 감사 자료에서 시간 정보를 이용하여 시스템 호출 순서 및 매개변수를 단위 시간으로 분할하는 기준을 의미한다. 이 때 시간의 단위는 ms를 사용한다. [그림 1]은 제안 모델의 구성요소이다. 구성요소는 크게 정상적인 시스템 호출 데이터 셋으로부터 침입탐지에 필요한 필드들을 추출하는 원시 데이터 수집 및 이벤트 생성 단계와 이 이벤트에 시간 개념을 적용하여 탐지자를 생성하는 학습단계, 새로운 프로세스가 실행되면 생성되는 시스템 호출 순서 및 매개변수에 시간 개념을 적용하여 학습단계에서 생성된 탐지자와 비교하여 시스템 호출 순서 및 매개변수의 길이에 대하여 비정상 유・무를 판단하는 침입탐지 단계로 이루어져 있다.

원시 데이터 수집 및 이벤트 생성 단계에서는 정상적인 데이터 셋과 공격이 이루어진 비정상적인 데이터 셋으로부터 시스템 호출 데이터를 수집하는 단계이다.

시간 기반 모델은 시스템 호출 순서의 비정상 유・무를 판단하기 위한 모델, 시스템 호출 매개변수 길이에 대하여 비정상 유・무를 탐지하기 위한 모델, 시스템 호출 순서만으로 탐지가 불가능하거나 시스템 호출 매개변수만으로 침입탐지가 불가능한 침입을 탐지하기 위해 시스템 호출 순서와 매개변수를 통합한 모델이다.

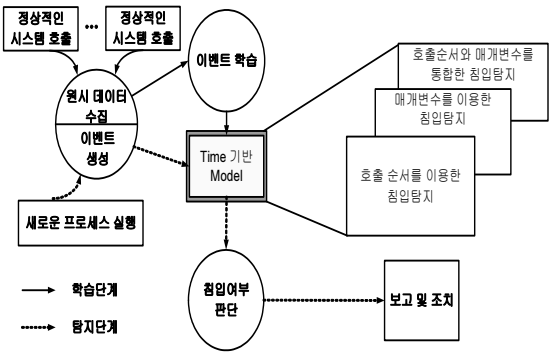

그림 1. 시간 기반의 침입탐지 시스템 개념도
Fig.1 Time based IDS

3.2. 시간 기반의 SCS의 비정상 행위 침입탐지 동작 과정

시간 기반의 시스템 호출 순서를 이용한 침입탐지 시스템의 처리과정은 [그림 2]와 같이 학습단계와 탐지단계로 구성한다.

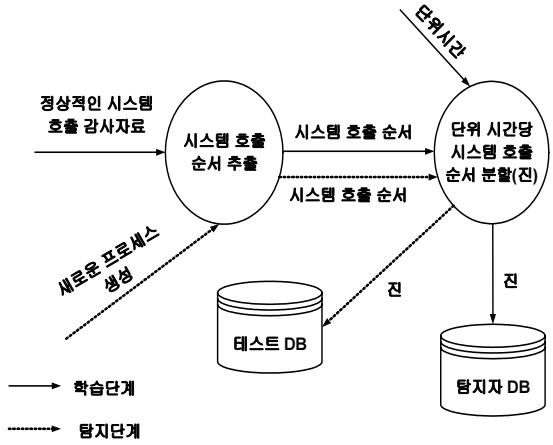

그림 2. 시간 기반의 SCS를 이용한 침입탐지 동작과정
Fig 2. Time based IDS using SCS

학습단계는 정상적인 시스템 호출 순서로 이루어진 데이터 셋을 시간 기반의 시스템 호출 순서를 이용한 침입탐지 시스템에서 필요한 필드들을 추출하는 시스템 호출 순서 추출 단계와 단위 시간을 적용하여 시스템 호출 순서를 분할하는 단계로 이루어져있다. 시스템 호출 순서 추출 단계는 시스템 호출 데이터에서 프로세스 ID, 시스템 호출 번호, 시간 정보를 추출하는 단계이다.

추출된 정보들은 단위시간 개념을 적용하여 시스템 호출 번호들을 단위 시간 간격으로 분할하고 이와 같이 분할된 시스템 호출 번호들을 진이라고 한다. 단위 시간을 적용하여 분할된 중복되지 않는 진들은 탐지자 데이터베이스에 저장되어 침입탐지자로 사용한다. 탐지 단계는 새로운 프로세스에 의해 생성되는 시스템 호출을 수집하여 비정상 유・무를 판정하는 단계로 시스템 호출 순서를 추출하는 단계, 단위 시간을 적용하여 시스템 호출 순서를 분할하여 진을 생성하는 단계, 학습단계에서 생성된 탐지자와 진을 비교하여 비정상 유・무를 판정하는 단계로 이루어져 있다. 시스템 호출 순서를 추출하는 단계는 새로운 시스템 호출을 수집하여 프로세스 ID, 시스템 호출 번호, 시간정보를 추출한다. 추출된 정보 시스템 호출 순서는 학습단계에서 적용한 단위 시간을 이용하여 진을 생성한다. 이와 같이 생성된 진은 학습단계에서 생성된 탐지자와 비교하여 비정상 유・무를 판정받는다.

3.3. 시간 기반의 SCP의 비정상 행위 침입탐지 동작 과정

시간 기반의 시스템 호출 매개변수를 이용한 침입탐지 시스템의 처리과정은 [그림 3]과 같이 학습단계와 탐지단계로 구성한다. 학습단계는 정상적인 시스템 호출 순서로 이루어진 데이터 셋을 시간 기반의 시스템 호출 매개변수를 이용한 침입탐지 시스템에서 사용하기 위해 필요한 필드들을 추출하는 시스템 호출 매개변수 추출 단계와 단위 시간을 이용하여 시스템 호출 매개변수를 분할하는 단계로 이루어져 있다. 시스템 호출 매개변수 추출 단계는 정상적인 시스템 호출 순서로 이루어진 데이터 셋에서 프로세스 ID, 시스템 호출 번호, 시간 정보, 매개변수를 추출하는 단계이다. 이와 같이 추출된 정보들은 시간 정보에 단위시간 개념을 적용하여 시스템 호출 매개변수들을 단위 시간 간격으로 분할하고 분할된 시스템 호출 매개변수들의 평균과 표준편차는 탐지자로 사용한다.

탐지 단계는 새로운 프로세스에 의해 생성되는 시스템 호출을 수집하여 비정상 유・무를 판정하는 단계로 시스템 호출 매개변수를 추출하는 단계, 단위 시간을 이용하여 시스템 호출 매개변수를 분할하여 매개변수 길이에 대한 평균을 획득하는 단계, 학습단계에서 생성된 탐지자와 전 단계에서 생성된 평균을 비교하여 비정상 유・무를 판정하는 단계로 이루어져 있다. 시스템 호출 매개변수를 추출하는 단계는 새로운 시스템 호출을 수집하여 프로세스 ID, 시스템 호출 번호, 시간정보, 매개변수를 추출한다. 추출된 시스템 호출 매개변수는 학습단계에서 적용한 단위 시간을 적용하여 분할 된 후 매개변수 길이에 대한 평균을 구한다. 이와 같이 생성된 평균은 학습단계에서 생성된 평균과 표준편차에 의해 비정상 유・무를 판정 받는다.

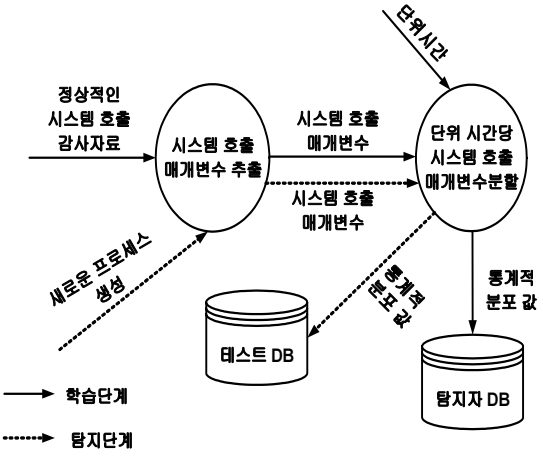

그림 3. 시간 기반의 SCP를 이용한 침입탐지 동작과정
Fig 3. Time based IDS using SCP

Ⅳ. 평 가

4.1. 개요

시간 정보를 이용하여 비정상 시스템 호출을 판단하는 시간 기반의 비정상 행위 침입탐지 모델을 실험하고 분석한다. 객관적인 실험 평가를 위해 시간 기반의 비정상 행위 침입 탐지모델에서는 1999년 DARPA 프로젝트에서 제공한 데이터[18]를 사용한다.

제안 모델의 실험을 위하여 사용된 실험 환경은 OS는 Windows XP SP2이고 1999 DARPA 데이터를 Visul C++ 6.0 컴파일러를 통해 감사 데이터를 추출한다. 긍정적・부정적 결함률을 개선하기 위한 기존 모델은 시그너처 기반, 데이터 마이닝 기법 등을 이용하거나 시스템 호출 순서를 일정 크기 단위로 분할하여 결함률을 개선하였지만 운영체제 및 네트워크 상태 등의 실험 환경에 따라 실험 결과가 다르게 나타났다. 따라서 제안 모델에서의

실험평가는 기존에 시간 개념을 적용한 연구가 충분하지 않으므로 DARPA 데이터에 대하여 시스템 호출 순서의 이상을 탐지하거나 매개변수의 길이가 정상적인 시스템 호출 매개변수의 평균적인 길이보다 큰 것을 비정상으로 판단하는 실험을 비교 평가한다.

[그림 4]는 실험 데이터 추출과정을 나타내고 있으며, 동작 과정은 운영체제에서 로그 파일을 생성하는 단계와 로그 파일로부터 실험에 필요한 데이터를 추출하는 단계로 구성된다. 실험 모델에서 사용되는 실험 데이터는 DARPA 로그 파일을 사용한다.

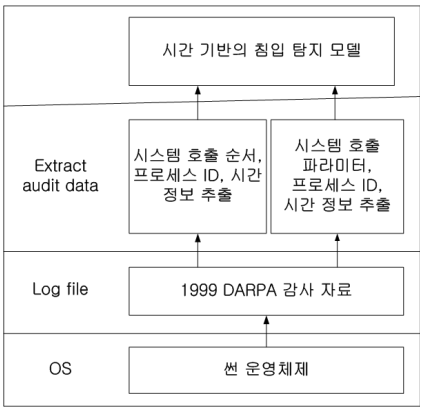

그림 4. 실험 데이터 추출 과정
Fig 4. Experimental Data

4.2. 실험방법

시간 기반의 시스템 호출 순서를 이용한 침입탐지 모델의 실험 시나리오-1은 시스템 호출 순서를 일정크기의 윈도우로 분할하여 침입을 탐지하는 기존 연구방법의 부정적・긍정적 결함률을 실험하고, 시나리오-2에서는 시간 기반의 시스템 호출 순서를 이용한 침입탐지 모델의 긍정적・부정적 결함률을 실험한다.

시간 기반의 시스템 호출 매개변수를 이용한 침입탐지 모델의 실험 시나리오-1은 시스템 호출 매개변수 각각의 길이에 대하여 침입을 판단하는 기존 연구방법의 부정적 결함률과 긍정적 결함률을 실험하고, 시나리오-2에서는 시간 기반의 시스템 호출 매개변수를 이용한 침입탐지 모델의 긍정적・부정적 결함률을 실험한다.

시간 기반의 시스템 호출 순서와 매개변수를 통합한 침입탐지 모델의 긍정적・부정적 결함률을 실험하고 각각의 제안 모델에 대하여 비교 분석한다.

4.3. 실험 결과

이 절에서는 시간 기반의 시스템 호출 순서를 이용한 침입 탐지 모델, 시간 기반의 시스템 호출 매개 변수를 이용한 침입 탐지 모델, 시간 기반의 시스템 호출 순서와 매개 변수를 통합한 침입 탐지 모델의 실험 결과에 대하여 기술한다.

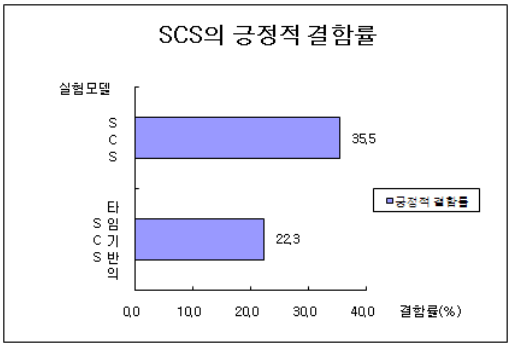

그림 5. SCS의 긍정적 결함률
Fig 5. False-positive of SCS

[그림 5]는 시간을 고려하지 않은 모델과 시간을 고려한 시스템 호출 순서에 대한 긍정적 결함률을 나타낸 것으로서 실험 결과 일정크기 단위로 시스템 호출 순서를 고려한 모델보다 시간 개념을 적용한 시스템 호출 순서 모델에서 긍정적 결함률이 13% 향상되었다.

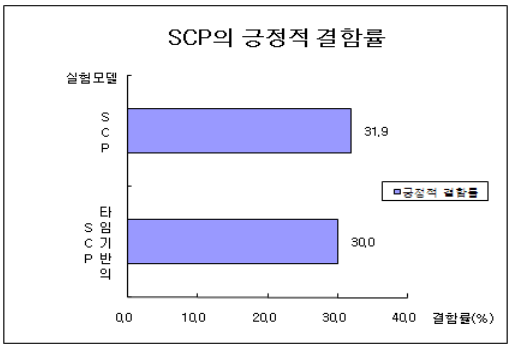

그림 6. SCP의 긍정적 결함률
Fig 6. False-positive of SCP

[그림 6]은 시간을 고려하지 않은 모델과 시간을 고려한 시스템 호출 매개변수에 대한 긍정적 결함률을 나타낸 것으로서 실험 결과 시스템 호출 매개변수 각각을 고

려한 모델보다 시간 개념을 적용한 시스템 호출 매개변수 모델에서 긍정적 결함률이 1.9% 향상되었다.

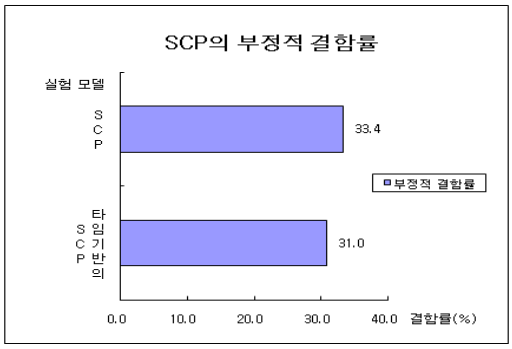

그림 7. SCP의 부정적 결함률
Fig 7. False-negative of SCP

[그림 7]은 시간을 고려하지 않은 모델과 시간을 고려한 시스템 호출 순서에 대한 부정적 결함률을 나타낸 것으로서 실험 결과 일정크기 단위로 시스템 호출 순서를 고려한 모델보다 시간 개념을 적용한 시스템 호출 순서 모델에서 부정적 결함률이 8.6% 향상되었다.

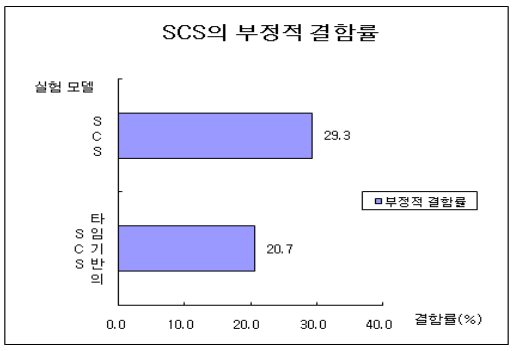

그림 8. SCS의 부정적 결함률
Fig 8. False-negative of SCS

[그림 8]은 시간을 고려하지 않은 모델과 시간을 고려한 시스템 호출 매개변수에 대한 부정적 결함률을 나타낸 것으로서 실험 결과 시스템 호출 매개변수 각각을 고려한 모델보다 시간 개념을 적용한 시스템 호출 매개변수 모델에서 부정적 결함률이 2.4% 향상되었다.

V. 결 론

최근까지 연구되던 침입탐지 모델은 시스템 호출 순서만으로는 침입을 판단하기 어려우므로 침입을 탐지하기 위해 시스템 호출 매개변수를 이용한 연구를 진행하고 있다. 이 논문에서는 시스템 호출이 발생하는 시스템의 긍정적 결함률과 부정적 결함률을 줄이기 위해 단위 시간 개념을 도입한 시간 기반 비정상행위 침입 탐지 모델을 제안하였다. 제안 모델은 DARPA 자료의 실제 침입 데이터의 시스템 호출 매개변수를 이용하여 침입을 판단할 때 시간 정보를 이용 하였다. 실험에서 시간을 고려하지 않은 시스템 호출 순서 모델보다 시간을 고려한 시스템 호출 순서는 긍정적 결함률에서 13% 향상되었고, 부정적 결함률에서는 9% 향상되었다. 시스템 호출 순서와 매개변수 길이에 시간을 고려한 제안 모델의 시간 복잡도는 $O(n^2)$이다. 향후 연구에서는 제안 모델이 기존 모델보다 비정상 시스템 호출을 정상으로 판단하는 긍정적 결함률과 부정적 결함률을 개선해서 탐지률을 높였지만 제공된 DARPA 감사 자료를 사용함으로써 수집된 데이터에 나타나지 않는 공격은 탐지할 수 없는 단점이 있다. 향후연구에서는 감사 자료의 추출방법 및 감사 자료에 모두 나타나지 않는 DOS 공격 등을 위해 매개변수 사이의 관계를 고려하여 성능을 향상시키기 위한 연구가 필요하다.

참고문헌

[1] S. Forrest, Steven A. Hofmeyr, Anil Somayaji, Thomas A. Longstaff, “A Sense of Self for Unix Process”, In Proc. of the 1996 IEEE Symposium on Research in Security and Privacy, Los Alamos, CA, pp. 120-128. IEEE Computer Society Press.

[2] J. B. D. Cabrera, L. Lewis, and R.K. Mehara. “Detection and classification of intrusion and faults using sequences of system calls”. ACM SIGMOD Record, Vol.30 No.4, 2001.

[3] G. Tandon and P. Chan. ″Learning rules from system call arguments and sequences for anomaly detection″. In ICDM Workshop on Data Mining for Computer Security (DMSEC), pp 20 - 29, 2003.

[4] G. Casas-Garriga, P. Diaz, and J.L. Balcazar. "ISSA : An integreated system for sequence analysis". Technical Report DELIS-TR-0103, Universitat Paderborn, 2005.
[5] 황현욱, 김민수, 노봉남, " 감사로그 상관관계를 통한 호스트기반의 침입탐지 시스템", 한국정보보호학회 논문지, 제13권 제3호, pp. 81-90, 2003.
[6] N.Ye and Q.Chen. "An anomaly detection technique based on a chi-square statistic for detecting intrusions into information systems". Quality and Reliability Engineering International, Vol. 17 No.2, pp. 105-112, 2001.
[7] C. Kruegel, D. Mutz, F.Valeur, and G. Vigna. "On the Detection of Anomalous System Call Arguments". In Proc. of the 2003 European Symposium on Research in Computer Security, Gjovik, Norway, Oct. 2003.
[8] 신미예, 전승흡, 이상호, "유전 알고리즘 기법을 이용한 HA 모델 설계", 컴퓨터정보학회 논문지 , 제14권 제10호, pp. 160 - 166, 2009.
[9] D. Wagner and P. Soto. "Mimicry attacks on host based intrusion detection systems". In ACM conference on Computer and Communications Security (CCS), 2002.
[10] S.Forrest, S. Hofmeyr and A. Somayaj, "Computer Immunology[review article]", In Communications of the ACM Vol. 40, No 10, pp. 176-187, 2007.
[11] 이종성, 채수환, "특권프로세스의 시스템 호출 추적을 사용하는 침입 탐지 시스템의 설계:면역 시스템 접근", 한국정보보호센터 '99 정보보호 우수논문집, pp. 181-206, 1999
[12] 이종성, "특권 프로세스의 시스템 호출 추적을 통한 침입 탐지:면역시스템 접근", 한국항공대학교, 2000.
[13] M. Markou and S. Singh, "Novelty detection : a review-part 1: statistical approaches", Signal Processing, Vol. 83 No. 12, pp. 2481-2497, 2003.
[14] Anil Somayaji and Stephanie Forrest. "Automated response using systemcall delays". In Proc. of the 9th USENIX Security Symposium, Denver, CO, Aug. 2000.
[15] 박봉구, "시스템 호출 기반의 사운덱스 알고리즘을 이용한 신경망과 N-gram 기법에 대한 이상 탐지 성능 분석", 인터넷정보학회논문지 제6권 제5호, pp. 45 - 56, 2005.
[16] 신미예, 원일용, 이상호, "타임 윈도우 기반의 T-N2SCD 탐지 모델 구현", 한국해양통신학회 논문지, 제13권 제11호, 2009.
[17] E. Tsyrklevich and B. Yee. "Dynamic detection and prevention of race conditions in file accesses", USENIX Security Symposium, Washington, DC, USA pp. 17-17, Aug. 2003.
[18] http://www.ll.mit.edu/mission/

저자소개

신미예 (Mi-yea Shin)

1990. 한밭대학교 전자계산학과 학사
1998. 충북대학교 대학원 전자계산학과 석사
2003. 충북대학교 대학원 전자계산학과 박사

※관심분야 : 암호이론, 정보보호, 네트워크보안, 정보검색

정윤수(Yoon-Su Jeong)

1998. 청주대학교 전자계산학과 학사
2000. 충북대학교 대학원 전자계산학과 석사
2008. 충북대학교 대학원 전자계산학과 박사

2008.3～2009.8 충북대 및 한남대 시간강사
2009.9～현재 한남대학교 산업기술연구소 전임연구원
※관심분야 : IPTV, 정보보호, 암호이론, Network Security, 유・무선통신보안

이상호(Sang-Ho Lee)

1976. 숭실대학교 전자계산학과 학사
1981. 숭실대학교 전자계산학과 석사
1989. 숭실대학교 전자계산학과 박사
1981. 3.～현재 충북대학교 전기전자컴퓨터공학부 교수

※관심분야 : 네트워크보안, Protocol Engineering Network Management