타임 윈도우 기반의 T-N2SCD 탐지 모델 구현

신미예*, 원일용**, 이상호***

Design of T-N2SCD Detection Model based on Time Window

Mi-Yea Shin*, Il-Young Won**, Sang-Ho Lee***

요 약

호스트 기반 침입탐지 기법에는 시스템 호출 순서를 고려하는 방법과 시스템 호출 파라미터를 고려하는 방법이 있다. 이 두 방법은 프로세스의 시스템 호출이 일어나는 전 구간에서 시스템 호출 순서에 이상이 있거나 시스템 호출 파라미터의 순서 및 길이 등에 이상이 있는 경우에 적합하지만 긍정적 결함율과 부정적 결함율이 높은 단점이 있다. 이 논문에서는 시스템 호출을 이용한 방법에서 발생하는 긍정적 결함율과 부정적 결함율을 줄이기 위해서 단위 시간을 도입한 타임 윈도우 기반의 T-N2SCD 탐지 모델을 제안한다. 제안 모델의 실험에 사용된 데이터는 DARPA에서 제공된 데이터이며, 실험 결과 제안 모델은 다른 시간 간격 보다 1000ms 시간 간격으로 실험하였을 경우가 긍정적 결합률과 부정적 결합률이 가장 낮았다.

ABSTRACT

An intrusion detection technique based on host consider system call sequence or system call arguments. These two ways are suitable when system call sequence or order and length of system call arguments are out of order. However, there are two disadvantages which a false positive rate and a false negative rate are high. In this paper we propose the T-N2SCD detection model based on Time Window in order to reduce false positive rate and false negative rate. Data for using this experiment is provided from DARPA. As experimental results, the proposed model showed that the false positive rate and the false negative rate are lowest at an interval of 1000ms than at different intervals.

키워드

침입탐지 시스템, 시스템 호출 순서, 인수 길이

Key word

Intrusion Detection System, system call sequence, argument length

* 충북대학교 전자계산학과 (제1저자)

** 서울호서전문학교 사이버해킹보안과 교수

*** 충북대학교 전기전자 컴퓨터공학부 교수 (교신저자)

접수일자 : 2009. 09. 04

심사완료일자 : 2009. 09. 29

Ⅰ. 서 론

침입탐지시스템(IDS: Intrusion Detection System)은 허가받지 않은 접근이나 해킹 시도를 감지하여 시스템 또는 망 관리자에게 통보 하고, 적절한 대응을 취하도록 하는 시스템을 말한다[1]. 침입탐지시스템은 감시 대상에 따라 네트워크 기반 IDS와 호스트 기반 IDS로 나눈다. 네트워크 기반 IDS는 실시간으로 네트워크를 감시하고 관리자가 정의한 보안정책을 적용하여 불법적인 침입에 대응할 수 있지만 실시간으로 패킷을 분석하고 처리할 수 있는 능력과 네트워크 트래픽 증가에 따른 하드웨어 및 소프트웨어의 구성이 필요하다. 호스트 기반 IDS는 별도의 하드웨어 없이 시스템을 감시할 수 있지만 서버마다 소프트웨어를 설치해야하므로 서버의 성능 저하를 가져올 수 있는 단점이 있다.

호스트 기반 비정상 탐지에 관한 연구는 Denning[2]의 연구를 시작으로 통계적 접근방법을 이용하여 비정상행위를 찾아내는 연구[3, 4]가 진행되어 왔다. 또한 호스트 기반 비정상 침입 탐지는 시스템 호출 번호 순서가 중요하므로 시스템 호출 번호 순서에 대한 변화를 이용하여 침입을 탐지하는 방법이 제안되었다[5-10]. 그러나 합법적인 시스템 호출 번호 순서를 모방 또는 흉내 내는 방법으로 악의적인 코드를 만드는 mimicry 공격 같은 경우는 시스템 호출 번호 순서만으로는 침입을 탐지하기 어렵다[11, 12]. 이러한 시스템 호출 번호 순서만으로 탐지하기 어려운 문제를 해결하기 위해 시스템 호출의 파라미터를 이용하는 방법들이 연구되었다[13].

시스템 호출 파라미터를 이용하는 기법들은 정상적인 시스템 호출 파라미터의 길이 및 통계적 분포를 이용한다. 대부분의 공격은 특정 시간에 시스템 호출 순서와 파라미터의 값에 변화가 있으므로 시간을 기준으로 시스템 호출 파라미터의 변화를 고려한다면 긍정적 결함율과 부정적 결함율을 낮출 수 있게 된다. 긍정적 결함률은 비정상적인 행위를 정상적인 행위로 판단하는 것을 의미하고, 부정적 결함률은 정상적인 행위를 비정상적인 행위로 판단하는 것을 의미한다.

이 논문에서는 침입 탐지를 효과적으로 수행하기 위해서 단위 시간을 중심으로 시스템 호출 번호 파라미터 길이의 통계적 특성을 고려한 비정상행위 침입탐지 기법을 제안한다.

제안된 기법은 단위 시간을 적용하여 시스템 호출을 ms 단위로 구분하고 구분된 각 구간의 파라미터에 대한 통계적 데이터를 분석함으로써 시스템의 긍정적 결함율과 부정적 결함율을 낮추었다.

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

Ⅱ. 관련 연구

이 절에서는 시스템 호출 번호를 이용한 방법과 시스템 호출 파라미터를 이용한 방법에 대해서 기술한다. 시스템 호출 번호를 이용한 방법은 시스템 호출 순서를 일정 크기 단위로 분할하여 불일치 률(mismatch rate)을 계산하여 침입 유·무를 판단하는 방법이고 시스템 호출 파라미터를 이용한 방법은 시스템 호출 문자열 파라미터 길이 값이 정상적인 행위의 시스템 호출 파라미터 길이의 평균보다 크면 침입으로 판단하는 방법이다.

2.1 시스템 호출 번호를 이용한 알고리즘

이 절에서는 시스템 호출 순서를 이용하여 침입을 탐지하는 기존 연구 방법에 대하여 기술한다.

2.1.1 negative selection

사람의 신체에서 항체를 생성할 때 흉선에서 T-세포가 생성되는 메커니즘을 이용한 negative selection은 정상적인 시스템 호출 순서를 적당한 크기의 윈도우로 분류한다. 이 윈도우 집합을 S라 부르고, 하나의 윈도우를 진(gene)이라 부른다. 윈도우 크기만큼 임의로 선택된 시스템 호출 순서의 집합 R_0는 S와 비교 후 일치하지 않으면 탐지자 R에 저장된다. 탐지 단계에서 이 탐지자에 해당되지 않은 시스템 호출은 비정상으로 판단하게 된다. 여기서 R_0는 1011011100110000에서 임의로 선택된 문자열을 의미한다. r-contiguous는 네거티브 셀렉션(negative selection)에서 S와 R_0를 비교할 때 연속해서

같은 것이 r개 있는지를 판단한다.

그림 1은 r-contiguous 방법으로 생성된 탐지자의 동작 과정을 보여준다. 그림 1에서 임의의 스트링(string) 1011011100110000을 하나의 시스템 호출 순서로 처리하는 것으로서 윈도우 크기 4로 진의 집합 S를 생성한다. S가 생성되면 임의의 문자열 R_0와 연속해서 2개(r=2) 일치되는 문자열이 있는지를 검사한다. R_0의 첫 번째 1000은 S의 첫 번째 1011에서 10이 연속하여 같으므로 탐지자에 포함될 수가 없으며, R_0의 두 번째 1100은 S의 마지막 0000에서 00이 연속하여 같으므로 탐지자에 포함될 수 없다[6].

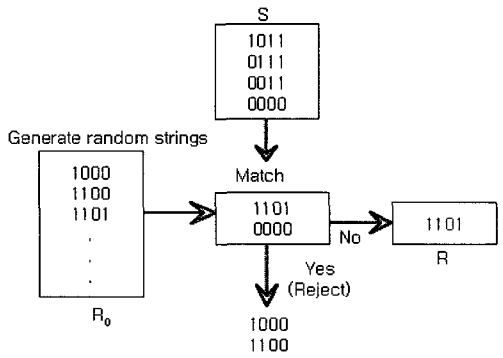

그림 1. r-contiguous 방법으로 생성된 detector
Fig 1. detector generation using r-contiguous

2.1.2 시스템 호출 번호 순서를 이용한 알고리즘

시스템 호출 번호 순서를 이용한 침입 탐지는 정상적인 시스템 호출 순서를 윈도우 크기만큼 분리하여 탐지자를 생성하고, 비교될 시스템 호출 번호 순서도 윈도우 크기만큼 구분하여 탐지자와 불일치 정도를 통계적인 방법으로 계산한다. k는 윈도우 크기 - 1이고, L은 시스템 호출 번호 개수일 때, 탐지자의 크기는 (식 1)과 같다[9].

$$k(L-k) + (k-1) + (k-2) + \cdots + 1 = k(L-(k+1)/2) \quad \text{(식 1)}$$

2.2 시스템 호출 파라미터를 이용한 알고리즘

mimicry 공격, security critical data공격, race condition 공격 같은 침입은 시스템 호출 번호 순서를 이용하여 판단하기가 어려우므로 시스템 호출 파라미터의 분포 및 순서 등을 이용하여 침입을 탐지하는 방법이 제안되었다[12].

시스템 호출 파라미터에 대한 평균 μ와 분산 σ^2을 갖는 문자열 길이 분포가 예측되어질 때, 시스템 호출 파라미터 모두에 대하여 길이 l을 갖는 파라미터 문자열의 평가는 (식 2)와 같이 Chebyshev inequality를 이용한다. 변수 x와 평균과의 차이가 임계치 t보다 클 가능성은 분산보다 작다.

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

$$p(l : l > \mu) = p(|x-\mu|) > |l-\mu|) < \frac{\sigma^2}{(l-\mu)^2} \quad \text{(식 3)}$$

문자열 길이 l이 평균 μ보다 클 가능성 $p(l)$은 (식 3)과 같다.

Ⅲ. T-N2SCD 모델

이 절에서는 단위 시간을 이용하여 시스템 호출 파라미터 길이의 통계적 특성을 고려한 T-N2SCD(Time based on Non-self System call Detection) 모델을 제안한다.

3.1 개요

T-N2SCD 모델은 DARPA 감사 자료에서 시스템 호출 번호, 시간, 파라미터 들을 추출하여 비정상 시스템 호출 유무를 판단하는 모델이다. T-N2SCD 모델은 침입이 일어난 구간에서 파라미터의 순서 및 길이의 변화가 정상적인 구간에서의 변화와 차이가 있다고 가정한다.

그림 2는 시스템 호출이 실행 될 때 필요한 정보 즉, 시스템 호출 번호, 시스템 호출이 시작된 시간, 파라미터의 개수, 파라미터 개수에 따른 파라미터를 수집하여 파라미터 길이에 대한 통계적 방법으로 시스템 호출이 정상적인지 아닌지를 판단하는 T-N2SCD 모델의 전체 동작 과정이다.

그림 2는 DARPA의 감사 자료에서 침입탐지에 필요한 요소를 추출하는 단계, 단위 시간 개념을 적용하여 매개변수의 길이를 분할하는 단계, 분할된 구간에 매개변수의 길이에 대한 평균과 표준편차를 이용하여 비정상

행위의 유·무를 판단하는 단계로 구성된다.

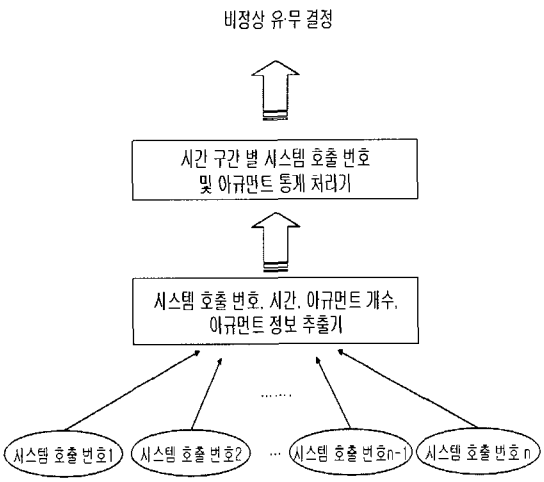

그림 2 시간 정보를 이용한 탐지 모델
Fig 2. Detection Model using time information

3.2 용어정의

T-N2SCD 모델에서 사용하는 주요 용어를 정의하면 표 1과 같다.

표 1. 파라미터
Table 1. Parameter

Notaion	Definitions
T_μ	정상적인 시스템 호출을 시간으로 구분한 모든 구간의 전체 평균
S_{avg}	정상 시스템 호출 파라미터의 시간 구간별 평균
R_{avg}	비정상 시스템 호출 파라미터의 시간 구간별 평균
F	비정상적인 시스템 호출 구간
D	S_{avg}의 원소들의 집합
d	R_{avg}의 원소들의 집합
d_n	비정상 시스템 호출에 대한 시간별 구간 개수
cnt	카운트 변수
μ	비정상 유무를 판단하기 위해 시간으로 구분한 모든 구간의 전체 평균
σ^2	비정상적인 시스템 호출에 대한 시간별 구간의 분산
X_i	시간으로 구분된 한구간의 평균

표 1에서 사용된 주요 파라미터는 정상행위 시스템 호출을 시간 개념에 적용하여 분할된 매개변수 길이의 평균 T_μ과 분산 σ^2을 이용한다. 새로운 시스템 프로세스가 실행될 때 생성되는 시스템 호출 매개변수는 단위 시간별 통계적 분포값 평균 μ를 계산하여 정상 행위의 시스템 호출로부터 생성된 평균과 분산을 이용하여 비정상 유·무를 판단하는 파라미터들이다.

3.3 T-N2SCD을 위한 시스템 호출 파라미터 추출

시스템 호출 파라미터는 시스템 호출이 발생할 경우에 이용될 호출 인자를 의미한다. T-N2SCD에서 시스템 호출 파라미터를 추출하는 과정은 그림 3과 같다. 그림 3은 원시 데이터를 파서를 이용하여 T-N2SCD에서 요구되는 정보를 추출하는 과정을 보여준다.

표 2는 그림 3의 과정 중에 DARPA에서 제공된 시스템 호출 데이터 중에서 T-N2SCD 모델에 필요한 정보만을 추출한 결과로써 시스템 호출 번호, 시스템 호출이 발생한 시간, 파라미터 개수, 파라미터 순으로 제안 모델에서 편리하게 사용하기 위해 praudit -r 명령으로 모든 데이터를 수치화한 것이다.

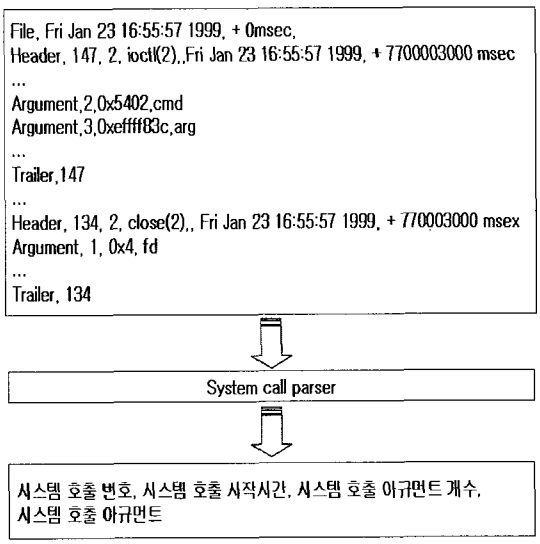

그림 3. 시스템 호출 파라미터 파싱
Fig 3. system call arguments parsing

표 2. 시스템 호출 파라미터 정보
Table 2. system call arguments information

시스템 호출 번호	시작시간(ms)	파라미터 개수	파라미터
113	920638412	0	
217	920638463	2	0x3, 0xefffdccc
158	920638463	0	
217	920638560	2	0x3, 0xefffdccc
158	920638560	0	
72	920638800	0	
· · ·	· · ·	· · ·	· · ·
26	920638800	1	0x0

3.4 T-N2SCD 모델 처리 과정

T-N2SCD 모델은 그림 4와 같이 정상적인 시스템 호출의 파라미터에 대한 시간 구간별 전체 평균 T_μ, 비정상 시스템 호출의 파라미터에 대한 시간 구간별 평균 μ과 분산 σ^2 그리고 비정상 시스템 유무 판단 등의 3단계 처리과정을 수행한다.

1단계에서는 정상적인 시스템 호출 시작 시간을 10ms, 50ms, 100ms, 500ms, 1000ms, 2000ms등과 같이 구분하여 각각에 대한 파라미터 길이의 평균 T_μ을 구하는 단계로써 시간 구간 100ms일 때 파라미터 통계는 표 3과 같다.

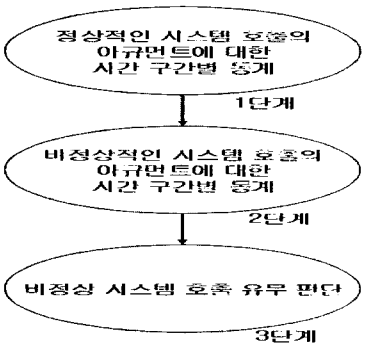

그림 4. T-N2SCD 처리과정
Fig 4. T-N2SCD process

2단계에서는 비정상 시스템 호출을 1단계와 같은 방법으로 시간을 구분하여 각각에 대한 파라미터 길이의 평균 μ와 분산 σ^2을 얻는 단계이다.

3단계에서는 표 3과 같이 정상적인 시스템 호출의 시간 구간별 평균 T_μ을 이용하여 2단계에서 얻은 평균 μ와 분산 σ^2을 이용하여 비정상적인 시스템 호출인지를 판단하는 단계이다.

표 3. 시간 구간별 파라미터 통계
Table 3. arguments statistic in time interval

시스템 호출 번호	시간 구간별 통계(100ms)		
	T_μ		
	T_1	$T_2 \sim T_{n-1}$	T_n
113	0	· · ·	0
217	9	· · ·	0
158	0	· · ·	9
72	0	· · ·	0
· · ·	· · ·	· · ·	· · ·
26	1	· · ·	2

표 4는 비정상 시스템 호출 유·무를 판단하기 위한 알고리즘이며 D와 d의 차이가 정상적인 시스템 호출의 구간별 모든 평균에 대한 평균보다 크면 비정상적인 시스템 호출 구간으로 판단한다.

표 4. 침입을 판단하기 위한 알고리즘
Table 4. algorithm to assess intrusion

$$
\begin{aligned}
&D := \forall time(S_{avg}) \\
&d := \forall time(R_{avg}) \\
&do \\
&\quad \text{if } diference(D, d, T_\mu) < (\frac{\sigma}{T_\mu})^2 \\
&\quad\quad then\ F := F \cup \{f\} \\
&\quad cnt := cnt + 1 \\
&endwhile(cnt < d_n) \\
&return\ F
\end{aligned}
$$

S_{avg} : 정상적인 시스템 호출의 시간 구간별 아규먼트 길이의 평균
R_{avg} : 비정상유·무 판단을 위한 시스템 호출의 시간 구간별 파라미터 길이의 평균
T_μ : 임계치 평균
F : 비정상적인 시스템 호출 구간

정상적인 시스템 호출에서 생성된 단위 시간으로 분할된 매개변수의 길이에 대한 평균 T_μ과 분산 σ^2을 새로운 시스템 호출이 실행되면 생성되는 시스템 호출 매개 변수의 길이의 단위시간별 평균 μ와 비교하여 평균 길이가 크면 침입으로 판단한다.

Ⅳ. 평 가

이 장에서는 시간 정보를 이용하여 비정상 시스템 호출을 판단하는 T-N2SCD 모델을 평가한다. 객관적인 실험 평가를 위해 N-N2SCD 모델에서는 DARPA 데이터를 이용한다[14]. DARPA 데이터는 2주간의 정상적인 시스템 호출 데이터와 3주간의 침입 데이터를 시간 정보에 의해 ms 단위로 구분하여 긍정적 결함율과 부정적 결함율을 최소화하는 가장 적절한 시간 간격을 찾는다.

4.1 실험 환경

표 5는 T-N2SCD모델을 실험 평가하기 위한 실험 환경을 나타내고 있다. DARPA 데이터는 OS 우분트(ubuntu)의 praudit 명령어를 이용하여 텍스트 파일로 가공 처리한 후 표 5와 같은 환경에서 T-N2SCD 모델을 실험 평가한다.

표 5. 실험 환경
Table 5. Experimental Environment

구 분	내 용
컴파일러	Visual C++ 6.0
메모리	1792MB
프로세서	AMD Athlon(tm)64* 2 Dual
OS	Windows XP SP2
데이터	DARPA 1999

4.2 실험방법

T-N2SCD 모델의 실험은 2주 동안 수집된 정상적인 DARPA 데이터를 이용하여 시스템 호출을 10CV에 따라 70:30의 비율로 1000회 반복 실험한다. 구분된 시스템 호출들은 호출 파라미터의 시간 정보에 대하여 10ms, 50ms, 100ms, 100ms, 300ms, 1000ms, 2000ms 등으로 구간을 정한 후 각각의 구간 안에서 파라미터 길이의 평균을 이용한다.

70%의 정상 시스템 호출에 대한 평균 T_μ와 30%의 정상적인 시스템 호출에 해당하는 파라미터의 길이에 대한 구간별 평균 μ와 분산 σ^2을 얻는다. 70%의 정상적인 시스템 호출 정보로 30%의 실험용 정상 데이터에 대하여 수식 4의 방법으로 긍정적 결함율을 구한다.

부정적 결함율은 70%의 정상 시스템 호출에 대한 평균 T_μ와 비정상 시스템 호출 파라미터를 동일한 방법으로 평균 μ와 분산 σ^2을 구하여 수식 4의 방법으로 부정적 결함율을 구한다.

$$p(|x_i - \mu| > T_\mu) < \frac{\sigma^2}{(T_\mu)^2} \quad \text{(식 4)}$$

표 6. 실험 결과 데이터
Table 6. Experimental Result Data

time 길이 (단위 ms)	정상파일 time구간 arguments	self-> nonself	false positive rate(%)	침입파일 time구간 arguments	nonself-> self	false negative rate(%)
10	2903	8	0.2756	18468	31	0.1679
50	1613	4	0.2480	10402	16	0.1539
100	2887	6	0.2078	18468	24	0.1299
300	3082	4	0.1298	19720	28	0.1420
1000	3279	3	0.0915	20951	27	0.1289
2000	3409	5	0.1467	21711	30	0.1382

4.3 실험 결과

표 6은 ms 단위로 정상적인 시스템 호출의 파라미터를 분리한 후 평균을 구한 값들에 대한 결과이다. 표 6에서 시간 간격을 1000ms(1초)로 하여 파라미터의 통계를 사용할 경우 긍정적 결합율과 부정적 결합율이 가장 낮았다. 반대로 표 6의 10ms나 2000ms처럼 시간 간격을 더 작게 하거나 더 크게 할 경우 T-N2SCD 모델에서는 긍정적 결합율과 부정적 결합율이 모두 높게 나타났다. 따라서 T-N2SCD 모델의 정상과 비정상 시스템 호출을 판단할 수 있는 시간간격은 1000회의 반복 실험을 통해 1000ms(± 50ms)이 가장 적합한 시간간격으로 나타났다.

표 6처럼 1000ms로 시간간격을 구분한 경우, 총 구간수는 3,279이고, 식 3에 의해 정상적인 시스템 호출을 비정상 시스템 호출로 판단한 구간은 3이어서 긍정적 결합율은 0.0915%이다. 비정상 시스템 호출에 대하여 1000ms로 시간간격을 구분한 경우 총 구간수는 20,951이고 비정상을 정상으로 판단하는 구간은 27이므로 부정적 결합율은 0.1289%이다. 이 같은 결과는 실험 환경이나 우분투(Ubuntu)와 리눅스에서 자체 수집한 실험 데이터에 따라 다르다[15].

V. 결 론

최근까지 연구되던 침입탐지 모델은 시스템 호출 순서만으로는 침입을 판단하기 어려우므로 침입을 탐지하기 위해 시스템 호출 파라미터를 이용한 연구를 진행하고 있다. 이 논문에서는 시스템 호출이 발생하는 시스템의 긍정적 결함율과 부정적 결함율을 줄이기 위해 타임 윈도우 기반의 단위 시간을 도입한 T-N2SCD 탐지 모델을 제안하였다. 제안 모델에서는 DARPA 자료를 이용하여 실제 침입 데이터의 시스템 호출 파라미터를 이용하여 침입을 판단할 때 시간 정보를 이용하는 실험을 하였다. 시간 간격을 1000ms로 구간을 결정하는 것이 긍정적 결합률과 부정적 결합률이 제일 낮음을 알 수 있다. T-N2SCD 모델은 시간을 이용하여 시스템 호출 순서 변화에 따른 침입 탐지 모델의 확장이 필요하다. 향후 연구에서는 시스템 호출 파라미터를 시간 간격으로 구분하여 통계처리한 모델과 시스템 호출 순서를 시간 단위로 구분한 모델을 통합할 계획이다.

참고문헌

[1] ETRI, 침입탐지시스템(IDS), 정보통신연구진흥원 학술정보 주간기술동향 1024호, Nov, 2001.

[2] D.E. Denning. An Intrusion-detection model. IEEE Transactions on Software Engineering, SE-13(2): 222-232, February 1987.

[3] Mark Burgess, Har다 Haugerud, Sigmund Straumsnes, and Trond Reitan. Measuring system normality. ACM Trans. Comput. Syst., 20(2):125-160, 2002

[4] 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, 17(2):105-112, 2001.

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

[6] Stephanie Forrest, Alan S. Perelson, Lawrence Allen, and Rajesh Cherukuri. Self-nonself discrimination in a computer. In SP '94: Proceedings of the 1994 IEEE Symposium on Security and Privacy, page 202, Washington, DC, USA, 1994. IEEE Computer Society.

[7] 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, 30(4), 2001.

[8] G. Casas-Garriga, P. Diaz, and J.L. Balcazar. ISSA : An integreated system for sequence analysis. Technical Report DELIS-TR-0103, Universitat Paderborn, 2005.

[9] S.A. Hofmeyer, A. Somayaji and S.Forrest, "Intrusion Detection Using Sequences of System Calls", Journal of Computer Security Vol. 6, pp. 151-180, 1998

[10] Anil Somayaji and Stephanie Forrest. Automated response using systemcall delays. In Proceedings of the 9th USENIX Security Symposium, Denver, CO, August 2000.

[11] D. Wagner and P. Soto. Mimicry attacks on host based intrusion detection systems. In 9th ACM Conference on Computer and Communications Security, Washington,

DC, pp. 18-22, Nov. 2002
[12] Chetan Parampalli , R. Sekar , Rob Johnson, A practical mimicry attack against powerful system-call monitors, Proceedings of the 2008 ACM symposium on Information, computer and communications security, March 18-20, 2008, Tokyo, Japan
[13] C. Kruegel, D. Mutz, F.Valeur, and G. Vigna. On the Detection of Anomalous System Call Arguments. In Proceedings of the 2003 European Symposium on Research in Computer Security, Gjovik, Norway, October 2003.
[14] http://www.ll.mit.edu/mission/
[15] 양대일, "정보 보안 개론과 실습", 한빛미디어, 2003.

저자소개

신미예(Mi-yea Shin)

1990. 한밭대학교 전자계산학과 학사.
1998. 충북대학교 전자계산학과 석사.
2003. 충북대학교 전자계산학과 박사 수료
※관심분야 : 암호이론, 정보보호, 네트워크보안, 정보검색

원일용 (Il-Young Won)

1998. 경원대학교 학사
2002. 건국대학교 석사
2006. 건국대학교 박사
2002.2.~2008.2. (주)사람과 사람들 이사
2005.2.~2008.2. : 신구대학 컴퓨터 정보과 겸임교수
2008.2.~현재 : 서울호서전문학교 사이버해킹 보안과 교수
※관심분야 : 보안, 인공지능,인공두뇌

이상호(Sang-Ho Lee)

1976. 숭실대학교 전자계산학과 학사.
1981. 숭실대학교 전자계산학과 석사.
1989. 숭실대학교 전자계산학과 박사.
1981. 3. ~ 현재 충북대학교 전기전자 컴퓨터공학부 교수
※관심분야 : 네트워크보안, Protocol Engineering, Network Management