제20회 한국정보처리학회 추계학술발표대회 논문집 제10권 제2호 (2003. 11)

성능 향상을 위한 통합 침입 탐지시스템에 대한 연구

홍성길*, 원일용*, 송두헌**, 이창훈*
*건국대학교 컴퓨터공학과
**용인 송담대학 컴퓨터소프트웨어학과
e-mail : : sunrise, clcc, chlee@konkuk.ac.kr
dsong@ysc.ac.kr

A Study on Combined IDS Model For Performance Improving

Seong-Kil Hong*, Il-Yong Won*, Doo-Heon Song**, Chang-Hun Lee*
*Dept. of Computer Science, Kon-Kuk University
**Dept of Computer Software, Yong-In Songdam College

요 약

네트워크 기반의 공격 및 비정상 행위를 정확히 탐지하고 판단하기 위한 기존의 탐지 모델은 공격 룰셋의 패턴매칭 기반인 Misuse Detection System을 사용하고 있다. 그러나 이 시스템의 특성상 새로운 공격의 미탐지 및 공격 오인등으로 False Positive 가 높다는 단점이 있다. 본 논문은 전체 시스템의 성능을 판정하는 False Positve 에러율을 줄여 성능을 향상하기 위해 Meachine Learning 기반의 Anomaly Detection System 을 결합한 새로운 탐지 모델을 제안하고자 한다. Anomaly Detection System 은 정상행위에 대한 비교적 높은 탐지율과 새로운 공격에 대한 탐지가 용이하다. 본 논문에서는 각 시스템의 탐지모델로 Snort 와 인스턴스 기반의 알고리즘인 IBL 을 사용했으며, 결합모델의 타당성을 검증하기 위해서 각 탐지 모델의 False Positive 와 False Negative 에러율을 측정하였다.

1. 서론

현재 네트워크 기반의 침입탐지 시스템은 네트워크를 통한 외부의 침입으로부터 내부의 특정 호스트들을 보호하기 위해 공격의 형태에 따라 미리 작성되어진 공격 시그네처(Signature) 매칭 기반의 Misuse Detection 방식을 사용하고 있다.

위의 시스템은 비교적 높은 탐지율을 보이고 있어 상용화 제품의 대부분이 Misuse Detection 모델에 기반을 두고 있다. 그러나 높은 탐지율에도 불구하고 공격 룰에 없는 새로운 공격이나 비슷한 유형의 우회적인 공격에 대해서는 탐지가 불가능 하다는 단점을 내포하고 있다. 또한 공격 룰과 유사한 정상적인 행위에도 불구하고 공격으로 오인하여 False Positive 를 빈번하게 발생하는 경우가 많으며, 새로운 유형의 공격을 탐지하기 위해서 주기적인 룰셋의 업데이트가 필요하다는 단점이 있다.

반면에 ML(Machine Learning)을 사용하는 Anomaly Detection 시스템은 정상인 학습 데이터를 이용 지식 패턴을 생성하고 이를 기반으로 공격 및 비정상행위를 탐지하기 때문에 정상적인 행위에 벗어나는 새로운 유형의 공격에 대해서는 기존의 Misuse Detection 기반의 시스템보다는 탐지가 용이하다.[2]

본 논문은 위에서 제기한 Misuse Detection 시스템의 단점을 보완하여 탐지성능을 향상 시키기 위한 방법으로 ML(Machine Learning)기반의 Anomaly Detection 시스템을 Misuse Detection 시스템에 결합하여 관리자에게 좀더 유연성 있는 Alert 정보를 제공 하도록 연구 및 실험하였다.

실험을 위한 Misuse Detection 모델로 Snort 를 사용했

다. Snort 는 오픈소스로 제공되며 다양한 공격 룰셋을 통한 공격 패턴 매칭 기술에 의해서 공격을 탐지한다.

Anomlay 시스템의 학습 엔진으로는 패킷 단위를 처리할 수 있는 인스턴스 기반의 IBL(Instance Based Learning)을 사용했다. 학습 알고리즘인 IBL 은 학습 데이터를 통해 지식 패턴을 생성하고 생성된 패턴을 바탕으로 비정상 행위를 구분한다.

2. 관련 연구

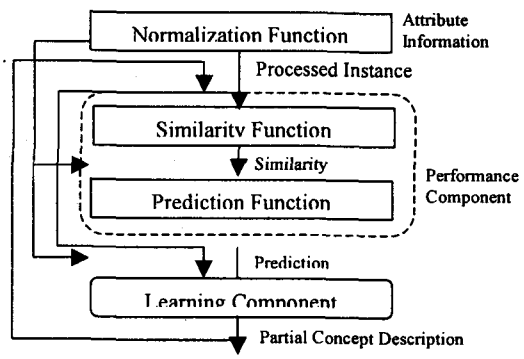
2.1 Snort (Misuse Detection)

무료 공개형 NIDS(Network Intrusion Detection System)로 대표적인 Misuse Detection 기반의 시스템이다. 다양한 공격의 룰셋을 포함하고 있으며, 패턴 매칭을 통한 탐지율도 높은 편이다.

Snort 의 탐지과정은 5 단계로 나눌 수 있다. 패킷을 탐지 할 Device 를 초기화하고 Open Packet library 을 이용 실시간으로 패킷을 캡쳐 버퍼에 저장하고 플러그인, 탐지 룰베이스, IP 헤더의 Prototype 및 이상유무를 체크하는 디코딩을 하며, 디코딩을 통한 분석자료를 기반으로 룰 베이스 패턴 매칭을 통해 탐지를 하게된다. 탐지된 Alert 은 Log 형태로 저장하며 관리자에게 보고하게 된다.

2.2 IBL(Anomaly Detection)

제안된 침입 탐지 시스템에서 탐지 모델의 생성기법은 하나의 사건을 설명할 수 있는 Instance 를 기반으로 하며, Instance 와 Instance 사이의 거리를 나타내는 유사도를 측정하여 패턴을 분류한다. 각 패턴은 PCD(Partial Concept Description)로 구성되며 하나의 PCD 는 패턴을 이루는 Instance 들 중 가장 높은 유사도와 해당 Instance 의 속성값들로 구성되며, 학습과정에서 생성된 PCD 는 하나의 Instance 를 처리할 때 마다 계속 업데이트함으로써 분리 패턴을 생성하게 된다. [1][4]



[그림 1] IBL 의 패턴생성 과정

IBL 의 학습과정은 3 단계로 분리되며 각 단계는 Instance 를 받아들여 일반화하여 학습을 위한 일반화된 Instance 를 생성하는 Processed Instance 를 생성하는 Pre-Process, 유사도 측정과 분류될 카테고리를 예측하기 위한 Prediction 을 생성하는 Performance Component, 다시 Processed Instance 를 받아들여 개념정보인 PCD 를 생성하고 이를 업데이트하는 Learning Component 로 구성된다.

모든 Instance 의 속성들은 Numeric value 또는 Symbolic value 로 채워진 속성값들로 구성된다. 이러한 Instance 의 속성값들 중 가장 높은 값과 가장 낮은 값을 탐색한 후 선택된 속성들을 제외한 모든 Instance 들은 linear normalizing 과정을 거치게 된다.[1][4]

$$Normalize\ \_attribute\ (x_a, a) = \frac{x_a - a_{\min}}{a_{\max} - a_{\min}}$$

위의 과정으로 일반화된 속성값들은 Performance Component 에 의해 Instance 사이의 관계를 설명하기 위한 유사도와 입력된 Instance 가 특정 카테고리에 속할 수 있는 예측치를 결정한다. 아래의 두 함수는 Similarity function 에 속하며 속성간의 거리를 측정하고 이것을 이용하여 속성사이의 유사도를 도출한다.

$$Similarity\ (x, y) = \frac{1}{\sqrt{\sum_{i \in p} Attribute\ \_defference\ (x_i, y_i)}}$$

$$Attribute\_difference(x_i, y_i) = (x_i - y_i)^2 \quad i\ is\ numeric\text{-}valued$$
$$= x_i \neq y_i \quad VDM$$

Similarity Function 에 의해서 계산된 유사도를 바탕으로 Instance 들을 묶고, 이렇게 묶인 k 개의 가장 유사한 Instance 들 중 가장 유사도가 높은 Instance 의 속성값들을 Learning Component 에게 넘겨 주는데 이때 이것을 Prediction 이라 한다. 이렇게 생성된 Prediction 을 기반으로 분류된 학습데이터에 대한 정보를 업데이트 한다.[1][3]

2.3 False Positive & False Negative

침입탐지시스템의 전체적인 성능을 가늠하는 척도는 False Positive 와 False Negative 의 에러율이다. False Positive 는 정상적인 행위에 대해서 탐지시스템이 이를 공격으로 오인하는 것이고, False Negative 는 행위가 공격임에도 불구하고 탐지시스템이 정상행위로 오인하는 것이다. 침입탐지 시스템의 주된 목적은 False Negative 의 에러율을 줄이는 것이지만, 현실적으로 불필요하게 많이 발생하는 False Positive 에러율의 문제가 대두되고 있다.[4]

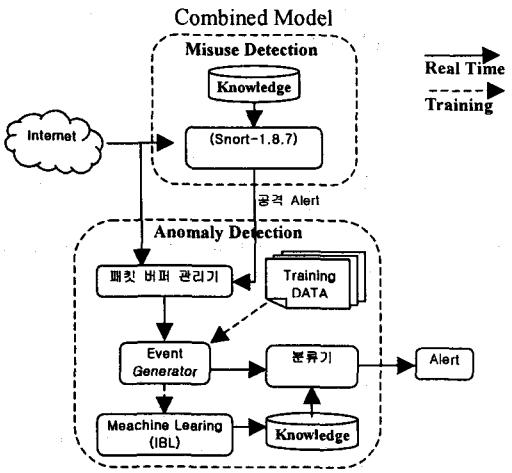
본 논문에서는 실험을 위해 다음과 같이 False Positive 와 False Negative 를 정의 하였다.

- False Positive 에러율 = 공격 Alert 수 / 전체 정상 Alert 수
- False Negavie 에러율 = 정상 Alert 수 / 전체 공격 Alert 수

본 논문은 Snort 와 IBL 의 에러율을 측정 각 시스템의 상호 보완된 결합이 적합할 수 있는지를 실험하였다.

3. 결합 모델 제안

본 논문에서 제안하고자 하는 시스템의 전체적인 시스템 구조도는 아래와 같다.



[그림 2] 결합 모델 구조

시스템은 크게 2 가지 부분으로 나뉘어져 있으며, 주 탐지 시스템은 Misuse Detection 기반으로 공격 탐지율이 비교적 우수하며 False Negative 에러율이 비교적 낮은 공인된 시스템인 Snort 가되며, 에러율를 줄이기 위해 결과의 정확성을 검증하는 보조 시스템으로 Anomlay Detection 시스템인 IBL 탐지 엔진이 적용되었다.

첫번재로, Anomaly Detection 시스템의 탐지엔진인 IBL 은 원시 학습 데이터에서 패킷을 추출하여 Event Generate 를 통해 학습을 하기 위한 Instance 를 생성하게 된다. 생성된 Instance Set 은 IBL 의 학습엔진을 통해서 지식을 생성하게 된다. 이렇게 학습에 의해서 생성된 지식은 추후 비정상 행위를 판단하는 근거자료로 사용하게 된다.

원시 데이터인 네트워크 패킷을 Misuse Detection 시스템인 Snort 에 보낸다. Snort 는 정해진 공격 룰과 비교분석을 한 후 공격유무를 결정하게 된다. 만약에, 패킷의 일정한 시점에서 Alert 이 발생하면, Snort 는 공격시간, 공격종류 등, Alert 의 정보를 보조 시스템인 Anomlay Detection 시스템에 있는 패킷 버퍼 관리기에 보낸다. 이때 발생한 Alert 이 False Positve 인지 아니면 실제 공격인지를 판단하기 위한 기준의 용이함을 제시하기 위해 보조 시스템인 Anomaly Detection 시스템의 평가를 받게 된다. Alert 이 발생한 시점을 기준으로 패킷 버퍼 관리기에 일정 시간동안 저장되어 있는 패킷을 침입판단을 위한 탐지 데이터로 사용하게 된다.

수집된 패킷은 Event Generator 통해 Instance 를 생성하게 되고 생성된 Instance 를 탐지 엔진인 IBL 의 학습기를 통해 미리 생성된 지식을 기반으로 분류기를 통해서 True Negative 및 False Positive 를 결정하게 된다.

IBL 은 Alert 정보를 탐지 확률(%)로서 표현하기 때문에 공격판단의 기준이 되는 Threshold(임계치)를 사용해서 판정한다.

4. 실험 및 분석

4.1 실험환경

본 논문의 실험환경은 PentiumⅢ-700, 리눅스 8.0, Snort 1.8.7 로 구성된 시스템과 Off-Line 기반에서 실시되었다.

실험에 사용되는 데이터는 공정성을 높이기 위해서 DARPA 산하 MIT Lincoln Lab.에서 제공하는 인증된 원시 패킷 데이터를 사용하였다. DARPA 는 1998 년부터 2000 년까지, 매년 다양한 공격행위 들이 포함되어 있는 약 7 주간의 tcpdump 데이터를 제공하고있으며, 본 논문은 1998 년도 7 주간의 training 데이터를 사용하였다.

4.2 실험용 데이터 및 가공

본 논문에서 사용하는 실험용 데이터는 Misuse Detection System 과 Anomaly Detection System 2 가지 종류의 데이터로 나누어진다. Misuse detection 모델은 Tcpdump 데이터로부터 수집된 순수한 원시 패킷을 사용하며, Anomaly 시스템은 IBL 학습엔진이 필요로 하는 Event 단위의 Instance 로 바꾸어야 하기 때문에 원시 패킷의 가공이 필요하다. 학습에 필요하는 정보 이외에 불필요한 다수의 자료가 있는데 이를 의미있는 정보 데이터로 축약할 필요가 있다. 이를 위해서 Event Generator 가 필요하게 된다. 센서는 패킷을 캡쳐한후 Event Generator 를 통해서 의미 있는 Event 형태의 Instance 로 변환하게 된다.

아래 [표]은 수집되는 데이터들로부터 비정상 행위를 구분하기위해 추출되는 판정 요소들이다.

종 류	속 성
TCP/IP	- 패킷 길이 - 패킷 유효시간 - 서비스 종류 - Protocol 종류 - Doff - WindowSize - 출발지 주소타입 - 목적지 주소타입 - 출발지 Port Type - 목적지 Port Type - 플래그 및 비트 : Fin,Syn,Rst,Psh,Ack - TCP 패킷 비율 : Inbound, Outbound

<표 1> Event 항목

실험을 위해서 Darpa 데이터 중 1 ~ 7 주차의 원시 패킷 Dump 데이터를 정상과 공격으로 나눈뒤 Attack Dump 데이터 중에서 Darpa 데이터의 공격 리스트를 참조 공격 유형별로 패킷을 추출 해냈다.

4.3 탐지 에러율 실험

새로운 결합 모델의 타당성을 검증하기 위해서 추출된 정상 데이터와 각 공격 유형별로 분류된 데이터로 Snort 와 IBL 의 True Positive, False Positive, True Negative, False Negative 에러율을 측정하였다.

구분	T.P	F.P	T.N	F.N
Snort	71%	29%	60%	40%
IBL	93%	6%	43%	56.8%

<표 2> Snort 와 IBL(T.P, F.P&T.N,F.N)결과

4.4 공격데이터에 대한 IBL 분석실험

각 주차 공격유형별로 추출된 총 82 개의 T.N 공격 중 정상 데이터에서 발생하는 F.P 와 공격명이 일치하는 23 개의 공격 data 에 대한 IBL 의 특성분석을 하였다.

공격명	패킷수	주차	IBL 판단		
			정상	비정상	탐지율
back	219	2_fri_back	195	24	10.95%
phf	7	6_mon_phf	2	5	71.42%
phf	7	7_wed_phf	6	1	14.28%
…	…	…	…	…	…

<표 3> 공격데이터 IBL 성능분석

4.5 정상 데이터에 대한 IBL 분석실험

주차별로 분류된 정상데이터에서 발생하는 73 개의 F.P 중에서 4.4 에서 사용한 공격명과 일치하는 24 개의 공격 data 대해서 분석하였다.

공격명	패킷수	주차	IBL 판단		
			정상	비정상	탐지율
back	4914	7_fri	4881	33	0.67%
phf	8	3_wed	3	5	62.5%
Phf	8	3_fri	7	1	12.5%
…	…	…	…	…	…

<표 4>False Positive IBL 성능분석

4.6 Threshold 측정

4.4 와 4.5 실험을 기반으로 Snort 를 거쳐 IBL 로 오는 Alert 데이터의 True Negative 와 False Positive 에러율을 줄이기 위한 Threshold 를 측정하였다.

공격탐지율(α)	T.N	F.P
25% ≤ α	19 개	11 개
50% ≤ α	19 개	8 개
70% ≤ α	18 개	0 개

<표 5>Threshold 측정

Threshold 의 기준값을 70%로 했을 때 적절한 성능을 낼 수 있을 것이라 예상된다.

4.7 성능분석

본 논문에서 제안한 결합 IDS 시스템의 성능에 대한 타당성을 제시하기 위해 Snort 와 IBL 에서 측정한 정확도 및 에러율을 기반으로 실험하였다.

모든 주차의 공격과 이에 상의하는 정상 데이터를 사용했으며 Snort 의 Alert 개수와 IBL 필터링을 결합한 통합된 시스템의 Alert 갯수를 체크하였다.

구분	T.N	F.P
Snort	83080 개	12945 개
결합 IDS	83060 개	30 개

<표 6> 결합모델 성능향상 분석 결과

위의 결과에서 결합 모델의 False Positive Alert 이 Snort 의 False Positive Alert 보다 97%이상 대폭 줄어든 것을 알수 있으며, TN 의 손실 또한 2%이내로써 실보다는 상대적으로 득이 많다는 것을 알 수 있다. Snort 에서 탐지한 공격 Alert 에 대해서 IBL 이 Threshold 를 통한 False Positive 를 필터링함으로써 탐지성능을 향상 시킬 수 있을 것이다.

5. 결론 및 향후과제

본 연구에서 Misuse Detection 시스템의 성능 향상을 위해서 Machine Learning 기법의 Anomaly Detection 시스템을 결합하여 상호보완함으로써 에러율을 줄여 시스템의 효율성을 증대 시킬 수 있는 방법을 제안 하였다.

문제점으로는 본 실험에서 사용한 데이터가 가상의 네트워크 환경기반에서 생성된 데이터를 사용함으로써 데이터의 무결성을 보장할 수 있지만, 실 네트워크 상에서는 Anomaly Detection System 에서 사용할 정상 데이터나 공격 데이터등에 대한 무결성을 검증하기란 쉽지 않을 것이다.

따라서 본 논문에서 제안된 시스템을 실 네트워크 환경에서 운영할 경우 우수한 성능은 보장할 수 없다.

향후 실험과제로 Snort 가 정상이라고 판단한 경우 실제 IBL 이 정상 탐지율이 높으므로 IBL 과 병합한다면 공격 탐지율을 높일 수 있을 것이다.

참고문헌

[1]David W. Aha, "A Study of Instance-Based Algorithms for Supervised Learning Tasks", Department of Information and Computer Science University of California, Technical Report , 1990

[2]J.Frank, "Artificial Intelligence and Intrusion Detection", NCSC, 1994

[3]김도진 "IBL 을 사용한 네트워크 기반 침입탐지 시스템과 평가 모델의 연구", 석사 학위 논문, 건국대학교 컴퓨터공학과 2003

[4]심철준 "침입탐지 시스템에서 Alert 의 패턴 학습을 이용한 False Positive 감소에 대한 연구",석사 학위 논문, 건국대학교 컴퓨터공학과 2003

[5]주대준 "데이터마이닝을 이용한 침입탐지 시스템의 설계 및 분석", 박사 학위 논문, 한국과학기술원, 2003