2001 년 한국정보처리학회 춘계 학술발표논문집 제 8 권 제 1 호

IDS 에서 Filter 와 Signature 의 역할에 대한 연구 (Date Mining 을 이용한 Feature Construction)

이정현*,원일용*,이창훈*
*건국대학교 컴퓨터공학과
e-mail : corona@konkuk.ac.kr clcc@ konkuk.ac chlee@konkuk.ac.kr

A Study for Filter and Signature on IDS (Feature Construction with Data Mining)

Jung-Hyun Lee*, Ill-young Weon*, Chang-Hun Lee*
*Dept. of Computer Engineering, Konkuk University

요 약

IDS 에서 가장 중요한 것은 침입을 논리적으로 모델링하고 , 이것을 센싱 할 수 있는 Filter 의 개발이며 Filter 에서 발생한 이벤트들에서 특정 공격 행위를 인식할 수 있는 신호인 Signature 의 정의를 통해 이벤트 스트림에서 Signature 를 자동으로 인식할 수 있는 방법에 대한 연구가 가장 핵심적이라고 할 수 있다.

본 논문은 이러한 filter 와 Signature 에서 사용할 수 있도록 특징들이 정의 되어있는 양식으로 원시 데이터로부터 profile 을 생성 filter 와 signature 에서 탐지할 수 있는 모듈을 적용할 수 있도록 네트웍과 host input stream 등의 raw audit data 에서 특징을 추출 Feature Construction 작성에 대한 연구이다.

1. 서론

최근 IDS(Intrusion Detection system)에 대한 연구는 활발하게 이루어 지고 있으며, 이미 시제품이 개발되어 그 사용의 범위를 넓히고 있다. 침입을 오용탐지(misused)와 비정상사용(anomaly) 탐지로 세분하고 있으며, 이러한 침입을 해석하고 인지할 수 있는 데이터베이스를 구축하고 있다. 이렇게 구축된 데이터 베이스는 IDS 연구에서 매우 중요한 부분 이라 할 수 있다. 국내의 경우 본 논문이 기고 되는 시점을 기준으로 100 여 개의 상용 비 사용 IDS 제품들이 발표되어 있으나 대부분의 제품들이 침입의 패턴에 대한 원천적인 연구가 부족하고, 외국의 유명 회사에서 구축해 놓은 데이터베이스와 이것을 인지하는 Signature 를 수입하여 국내의 컴퓨터 환경에 적합하도록 최적화 시켜놓은 정도가 주를 이루고 있다.

IDS 에 대한 연구는 그 근원을 1980 년대 초반으로 추정하며 본격적인 연구는 1990 년대에서부터 시작 되었다. 1996 년을 기점으로 DARPA 를 중심으로 IDS 에 관련된 표준화의 움직임이 시작 되었으며 현재는 연구기관 중심의 표준화와 상용제품을 주도하는 회사들의 컨소시엄을 중심으로 하는 표준화가 각각 다른 방향에서 진행되고 있다[IDWG, CIDF, ISO/IEC JTC1/SC27 WG1,etc].

IDS 에 대한 연구는 점차적으로 anomaly 탐지 방향으로 연구가 진행되고 있고, 어느 정도 연구가 이루어 졌다.

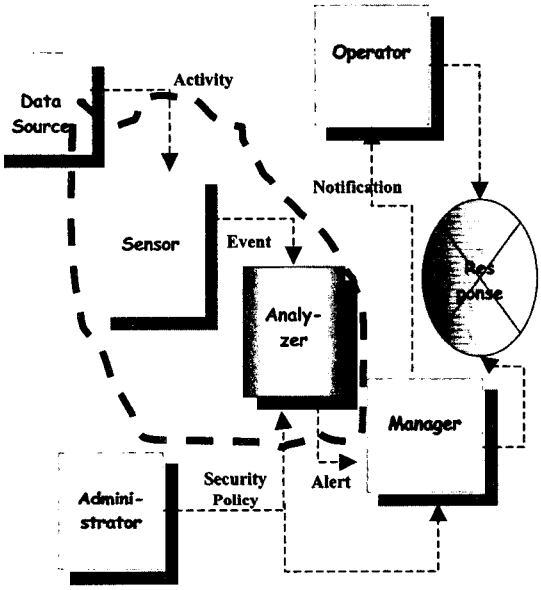
본 논문은 이러한 탐지에서 사용할 수 있는 데이터를 생성하기 위해 network traffic 뿐만 아니라 호스트에서 발생하는 input stream 을 통해서 각각의 profile 을 생성하여 침입탐지 모듈에 적용할 수 있는 Feature Construction 을 생성하는데 그 목적이 있다. 먼저 2 장 IDS Models 에 대한 설명이다. 3 장은 Data Mining 기법을 이용한 Feature Construction, 마지막으로 4 장은 그 적용 실험을 하였다.

2. IDWG 의 IDS Models

IDS 에서 원시자료는 네트웍기반이 경우 네트웍의 원시 패킷이 될 것이며, 호스트 기반인 경우 System call(System command)의 순서와 그 parameter, Input stream, Application 인 경우 그 Application 이 만들어 놓는 Log file 이다.

본 논문의 용어는 IDWG 에서 사용하는 용어를 기본으로 사용한다.

IDWG(Intrusion Detection Working Group)가 정의 하는 IDS 의 핵심적 구성 요소는 <그림 2.1>과 같다.



<그림 2.1> IDS 의 구성요소 (IDWG 기준)

침입은 각각의 경우 적당한 원시자료에 일부분으로 발생하게 된다. 센서는 이러한 원시자료를 감시하는 모듈로 IDS 운영자가 감시하고자 하는 이벤트를 정의해 놓은 것에 의하여 원시자료가 특정 조건을 만족하는 경우 이벤트로 만든다. Analyzer 로 보내고 이러한 이벤트 중 특정 조건을 만족하는 이벤트들의 집합에서 침입의 흔적 즉 Signature 를 발견하고 침입 판단 여부를 결정한다.

만약 이벤트의 집합 중 침입을 발견하게 되면 Manager 에게 통보(Alert)를 하고 Manager 는 관리자에게 통보하고 침입에 대하여 대응을 하게 된다.

2.1 Sensor 와 Filter

Sensor 는 원시자료를 읽고 분석할 수 있는 IDS 의 모듈로서 원시 자료 중에서 특정 조건을 만족하는 자료만을 다시 가공하여 분석기로 보내는 역할을 한다. 이때, 원시자료에서 원하는 자료만을 선별하는 기준이 되는 것을 필터라고 한다. 필터는 일반적으로 특정한 규칙을 가지고 있으며 일반적으로 이 규칙은 간단하다. 필터는 자신의 조건을 만족시키는 원시 자료를 제 가공하는데 이렇게 제 가공된 자료를 이벤트라고 부른다.

한 개의 target 에 대한 공격은 일반적으로 한 개 이상의 필터로 되어 있으며 특별한 경우에는 n 개의 필터로 구성 될 수도 있다. 또는 한 개의 필터가 n 개의 이벤트와 관련될 수도 있다. 즉 이러한 것은 센서와 필터를 설계 하는 설계자의 의도에 달려 있는 것이다.

2.2 Event 와 Audit trail

Event 는 Sensor 에서 Data Source 중 Filter 에 의해서 특정한 모양으로 가공되어진 자료를 의미 한다. 원시자료가 필터을 통해 이벤트로 가공되었다는 것은 이미 관심 있는 특정 자료만으로 감시해야 할 자료의 범위를 축소 했다는 의미를 갖는다. 이러한 Event 들의 연속된 stream 을 Audit trail 이라고 한다.

일반적으로 알려진 Audit trail 은 원시자료의 기록으로 보는 시각도 있지만, 각각의 OS 레벨에서 사용하는 audit trail 은 IDS 에서 사용하는 Audit trail 과는 다른 의미로 사용된다. 그러나 OS 레벨에서 만들어진 Audit trail 을 Sensor 없이 바로 Analyzer 에서 사용한다면 이 자료는 이미 이벤트의 연속으로 볼 수 있으므로 이때는 IDWG 의 Audit trail 과 같은 의미를 같게 된다.

2.3 Analyzer 와 Signature

Signature 는 연속된 이벤트의 스트림 중 특정한 패턴을 의미 하며 이 패턴은 침입판단 여부의 근거가 된다. Analyzer 는 이벤트들의 연속된 스트림에서 signature 를 찾아내는 기능을 하는 IDS 의 모듈이다.

Analyzer 가 Signature 를 인식하는 방법에는 여러 알고리즘이 있으며 주로 전통적인 AI 에서 추구하는 패턴 매칭 기법들의 변형들이 주류를 이루고 있다. 그러나 기존의 방법을 그대로 사용하기에는 약간의 무리가 따르는데 그 이유는 도메인의 차이에 의한 패턴의 특성 때문이다. 이러한 패턴의 특성이 Signature 를 찾아내는 방법을 결정한다.

2.4 이벤트 발생과 Alert

센서가 이벤트를 만든 후 그 자료를 분석기에 넘기는 동작을 이벤트를 발생시킨다라고 한다. 그리고 분석기에서 특정 공격의 징후인 Signature 를 인식한 후 Manager 에게 침입을 알리는 과정을 Alert 라고 한다.

지금까지의 대부분의 IDS 는 센서와 분석기의 분리가 명확하지 않았으며 이 두 부분이 통합되어 있어서 이벤트 발생과 Alert 의 개념이 혼합되어 있어서 Alert 가 이 두개의 개념을 모두 의미 하기도 하였으나, IDWG 방법으로 접근 하면 모두 해석이 가능하다.

Data Source 에서 특정 조건을 만족 시키는 Data 인지를 판단하는 Sensor 부분에는 조건을 검사하는 것이 필터라고 할 수 있다. 그리고 Signature 는 특정한 이벤트들의 집합이며 이것은 패턴의 형태이고 이 Signature 를 감지하는 모듈이 Analyzer 에 있으며 패턴 감지 시 특정한 알고리즘을 사용하게 되는 것이다.

3. Data Mining 를 이용한 Feature Construction

2 장에서 Analyzer 와 Signature 에서 필요한 데이터 수집 필요하고, IDS 가 탐지를 하는 대상분류에서 네트웍과 호스트를 서로 분리해서 다른 접근 방식으로 데이터를 수집하지만 실제 Feature Construction 은 기본적인 데이터를 제공하는데 쓰여진다.

Feature Construction 은 raw audit data 로부터 네트웍 및 호스트에서 많이 사용되는 특징들을 추출하여 저장하여 시켜 놓은 데이터 테이블이다.

3.1 특징 추출위한 Data Mining Algorithms

Feature 는 Audit Data 로부터 탐지 모델에서 사용할 데이터를 추출하는데 있어 필요한 정의된 필드를 말한다. 정의된 필더를 가져와 연관규칙과 Frequent Episodes 를 이용하여 Feature Construction 만든다.

연관규칙과 Frequent Episodes 알고리즘은 엄청난 양의 data 에서 필요한 데이터를 많은 추출하는데 매우 효율적인 알고리즘이다.

3.1.1 연관규칙

마이닝 연관 규칙의 목표는 Audit data 테이블로부터 다중 Feature 들을 가져 오는 것이다. Audit data 가 주어졌다고 가정했을 때, *support*(X)는 X set 에 포함되어 있는 data 의 비율로 정의한다.

- 연관규칙은 $X \rightarrow Y, [c, s]$, [8]
- X,Y item sets ,
- $X \cap Y = \emptyset$,
- $s = support(X \cup Y)$
- $c = \frac{support(X \cup Y)}{support(X)}$

이다.

여기에서 비교대상이 되어지는 데이터는 이미 정상 사용자 프로파일로 정의 되어 있어야만 가능하다.

3.1.2 Frequent Episodes

시간이 표시되어 있는 event record 들이 주어져 있을 경우 Interval[t_1, t_2] 는 두개의 이벤트 레코드는 시작 Timestamp t_1, 끝 Timestamp t_2 의 이벤트 레코드의 순차이다.

Support(X)는 전체 이벤트에서 X 가 포함된 것이 최소한 발생한 빈도이고,

- Frequent Episodes rule 는 $X,Y \rightarrow Z, [c, s, w]$, [8]
- X,Y,Z 은 Item sets 이고,
- $s = support(X \cup Y \cup Z)$,
- $\frac{support(X \cup Y \cup X)}{support(X \cup Y)}$ c=
- w

4. 사례를 통한 실험

Raw Audit Data 는 BSM 을 통해서 얻어진 tcpdump data 이며 content(data)를 기본적으로 갖고 있다. Feature construction 을 만들기 위해서는 Network 의 Feature 과 Host 일 경우가 Feature 의 Feature 가 다르기 때문에 각각의 Feature 를 3.1 절 Data Mining 알고리즘을 통해서 Feature Construction 를 만든다.

4.1 네트웍에서의 Feature Construction 적용

네트웍 기반 침입은 그 유형이 매우 다양하며, 짧은 주기고 계속해서 변하고 있다. 하지면 탐지 시스템입장에서 4 가로 분류 할 수 있다.

- DOS, 서비스 거부 공격, 예를 들어 ping-of-death, teardrop, smurf, synflood 등등
- R2L, 원격에서 권한 없는 접속, 예를 들어 비밀번호를 계속 바꾸어 치는 행위
- U2L, 권한이 없는 내부사용자가 내부 슈퍼유저 권한으로의 권한 없는 접속, 예를 들어 다양한 버퍼오버플로우 공격
- PROBING, 어떤 위협이나 탐지, 예를 들어 port-scan, ping-sweep 등

label	service	host_count	host_rej_%	host_diff_srv%
normal	ecr_i	1	0	1
smurf	ecr_i	350	0	0
satan	user_level	231	85%	89%
normal	http	1	0	1
...	...	...	...	...

<표 3-2-1>네트웍 접속 레코드의 Feature Construction[8]

smurf 공격의 경우 네트웍 Feature 에서 host_count >5 회일 경우 DOS 공격으로 하나로 간주한다. 그리고 satan 의 경우 host_rev > 83% and host_diff_srv > 87%이상의 경우 PROBING 공격의 일종으로 탐지 되었다.

여기에서 DOS 와 PROBING 공격은 Frequent Episodes 에서 time window 안에 일정한 공격 패턴이 반복되어 이를 탐지 할 수 있지만 R2L 과 U2L 같은 경우 전혀 패턴일 있을 수 없다. 이런 유형의 공격은 한번의 실행으로 타겟에 치명적인 피해를 가할 수 있다. 따라서 네트웍에서의 Feature 는 TCP/IP 패킷을 fields 뿐만 아니라 그 Data 의 Content 를 Feature 로 추출하여 profile 을 생성하였다.

또한 이러한 특징들로는 Login 의 실패횟수, Login 성공 여부, 루트로 Login 했는지, 루트 권한을 획득했는지, 접속 제어 파일(/etc/passwd, .rhosts)등에 대한 접근 횟수등 content 에 대한 Feature 를 추출할 수 있는 함수를 포함 해야 한다.

4.2 호스트에서의 Feature Construction 적용

내부에서 일어나는 침입을 차단하기 위해서 IDS 는 호스트 발생하는 각 사용자의 key stroke 등의 input stream, System call, cpu 이용률 등을 특징으로 잡고 추출하여 3.1 절에서 언급한 알고리즘을 통해 Feature

Construction 를 작성한다.

Time	hostname	command	Argv1	Argv2
am	under	mkdir	dir1	
am	under	cd	dir1	
am	under	vi	tex	
am	under	tex	vi	
am	under	mail	fredd	
am	under	subject	progress	
am	under	vi	tex	
am	under	vi	tex	
am	under	mail	fredd	
...	..	...	...	...
am	under	vi	tex	

<표 3-2-2>호스트 Shell Command Records[8]

호스트에서 정의 되어 질 수 있는 Feature 은 <표 3-2-2>과 같다고 가정할 때 Shell Command Records 들로부터 연관 규칙을 이용하여 Feature Construction 을 만들 수 있다.

예를 들어 명려어 vi → tex = am, hostname = under, argl = tex,[1.0,0.28]

100% under tex

. data 28%

Feature Construction

5. 결론 및 향후 과제

IDS 에서 수많은 원시자료를 효율적으로 필터링하기 위해서는 시간과 비용이 항상 딜레마이다.

많은 원시 자료를 빠르고 효율적으로 다루기 위해 본 논문에서는 데이터 마이닝 기법들을 이용한 Feature Construction 알고리즘을 제안 하였다. 제안된 알고리즘은 호스트기반 및 네트웍 기반에서 모두 적용가능하다. 데이터 마이닝과 관련된 연관규칙과 Frequent Episodes 을 이용하여 알고리즘을 생성 하였다. 또 간단한 사례를 통한 실험 결과를 보였다.

추후 제안된 알고리즘의 실용성과 효용성의 증명을 위하여 실험실 환경이 아닌 실제 환경에서 일정기간 실험이 필요하다. 호스트 및 네트웍 기반실험으로 구분하고, misuse 와 anomaly 에 각각 적합하도록 알고리즘의 최적화가 필요하다.

참고문헌

[1] Stephan Northcutt, Judy Novak,Donald mcLachlan "Network Intrusion Detection An Analyst's Handbook", second Ed, New Riders September,2000

[2] 김주영, 강창구,이극, 이소우 "네트워크 패킷 분석을 통한 침입탐지 기법 개발",1999

[3] 성승제, 강창구, 소우영 "네트워크 기반 실시간 침입탐지시스템을 위한 감사자료 수집모듈 설계 및 구현",1999

[4] Jean-Philippe Pouzeol , Mireille Ducasse "Handling Generic Intrusion Signatures",2000

[5] Steven T. Eckmann , Giovanni Vigna , Richard A. Kemmerer "STATL: An Attack Language for State-based Intrusion Detection ",1999

[6] Giovanni vigna , Richard A,Kemmerer "NetSTAT: A Network-based Intrusion Detection Approach",1999

[7] A Data Minig Framework Framework for Building Intrusion Detection Models,199x

[8] R. Agrawal, T.Imielinski, and A. Swami. Mining association rules between sets fo items in large database.1993