제21회 한국정보처리학회 춘계학술발표대회 논문집 제11권 제1호 (2004. 5)

추론망 자동 생성기법을 이용한 비정상 침입탐지

김찬일, 김민경, 신화종
한국정보보호진흥원
e-mail : chankim@kisa.or.kr, mkkim@kisa.or.kr, shinhj@kisa.or.kr

Anomaly Detection Using the Automatic Creating Inference net Method

Chan-il Kim, Min-kyung kim, Hwa-jong Shin
Korea Information Security Agency

요 약

기존의 침입을 탐지하는 방법은 여러 가지가 있지만, 모든 침입을 다 탐지하지는 못하고 있다. 공격자는 알려지지 않은 취약점을 이용하거나 취득한 패스워드나 ID 계정을 이용하여 공격하고자 하는 시스템에 악의적인 행위를 한다. 이런 침입을 탐지하는 연구는 탐지엔진에 적용될 패턴구성 방법이 핵심이다. 본 논문에서는 기존의 사람이 패턴을 찾는 것을 자동화 시키고, 자동화된 패턴 구축 방법을 직접 시스템에 적용하여 침입을 탐지하는 방법을 제시하고자 한다. 그래서 알려지지 않은 침입을 탐지하기 위해 전문가 시스템을 이용하고 패턴을 지식 베이스화하는 작업과 그 지식을 추론할 수 있는 추론망을 추론망 자동 생성 기법으로 구성하여 비정상적인 침입을 탐지하는 방법을 본 논문에서 제시하고자 한다.

Key words : Anomaly Intrusion Detection, Expert System, Inference net

1. 서론

침입탐지시스템은 침입을 탐지하여 대응하여 피해를 최소화하는 대응책으로서 유용성과 그 가치가 인정되어 정보보호의 중요한 기술 요소로 인식되고 있다[1]. 이러한 침입탐지시스템에는 외부 또는 내부에서 유통되는 시스템의 정보를 분석하여 침입을 탐지하고, 탐지결과를 관리자 또는 이 결과를 필요로 하는 다른 사용자에서 알려주는 기능과 사후에 이 침입에 대한 정보를 분석 할 수 있도록 로그를 남기는 감사 기능이 있다[2].

본 논문에서는 비정상적인 침입탐지 방법 중 예측 가능한 패턴 생성 (Predictive Pattern Generation) 방법의 일부분으로 예측 가능한 패턴을 추론망 자동 생성 기법으로 패턴들을 만들고 전문가 시스템이 침입 여부를 결정하는 방법을 제시하고자 한다.

2 장에서는 현재 비정상적인 침입탐지 방법의 분류와 탐지 방법에 관하여 간략히 기술하고 3 장에서 전문가 시스템에 대한 전반적인 개요와 추론망의 정의와 추론망이 전문가 시스템에 구축에 어떤 역할을 하는지 기술한다. 4 장에서 자동추론망 생성 기법의 필요성과 추론망 자동 생성 기법을 적용하기 위하여 사전에 준비할 사항을 기술하고 5 장에서는 추론망 자동 생성 기법을 생성된 추론망을 이용한 비정상 침입탐지 방법을 시스템에 직접 적용하여 구현한 예를 보여준다. 6 장에서 본 시스템의 장단점과 한계에 관하여 기술하여 결론을 내린다.

2. 비정상 침입탐지 방법

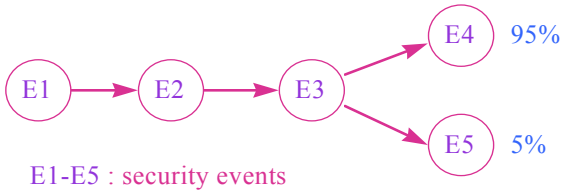
비정상적인 침입 탐지 방법의 종류는 다른 시점 다른 견해로 나누어져 그 종류를 정의하고 하고 있다. 가장 최근에서 ACM 에서 모든 것을 통합 분류하여 3 가지 정도로 분류하고 있으며, 국내에서는 KISA 에서는 2000 년도 정보통신 기반구조 보호기술에서 5 가지 종류로 분류하고 하고 있다.

비정상적인(anomalous) 침입 탐지 방법의 종류

- 통계적인 방법 (Statistical approaches) : 통계적인 방법은 비정상적인 침입의 탐지를 주로 통계적으로 처리하는 방법이다.
- 특징 추출 (Feature Selection) : 특징 추출은 특

정 침입 패턴을 추출하는 방법이다.

- 비정상적인 행위 측정방법들 (anomaly measures)의 결합 : 이 방법은 여러 비정상적인 행위 측정 방법들을 사용하여 각각의 결과를 통합하여 특정 행위가 정상인지 비정상인지를 측정하는 방법이다.
- 예측 가능한 패턴 생성 (Predictive Pattern Generation) : time-based rule 을 사용하여 각각의 이벤트에 시간을 부여할 수 있으며, 이벤트의 순서가 올바른 경우에도 시간의 간격에 따라 주어진 이벤트들이 정상인지 비정상인지 탐지할 수 있다.



<그림 1> 예측 가능한 패턴 생성

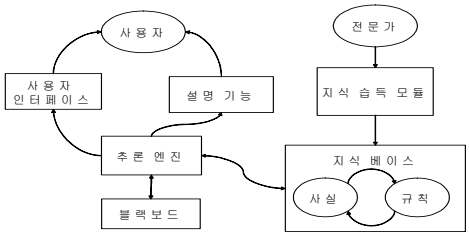
- 신경망 (Neural Network) : 이 방법은 명령어의 순서를 신경망으로 학습시켜서 다음에 수행될 명령어를 미리 예측하여 비정상적 침입을 탐지하는 방법이다.

3. 전문가 시스템과 추론망

전문가 시스템은 적용 영역의 전문가들이 가지고 있는 전문 지식을 지식베이스로 구축하여 저장함으로써 컴퓨터가 전문가의 기능을 인간과 같은 논리적인 사고로 대신 수행케 하는 시스템이다.[2, 3]

3-1 전문가시스템의 구성요소

전문가시스템은 지식베이스, 추론엔진, 작업메모리, 사용자 인터페이스 등의 요소로 구성되어 있다. 이들간의 관계를 보여주고 있다. [9]



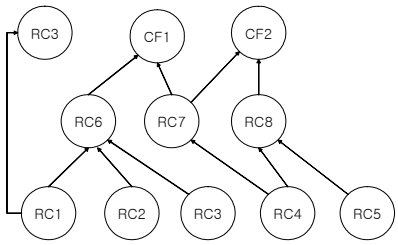
<그림 3> 전문가 시스템 구성 요소

3-2 추론망

규칙 기반 시스템(Rule-based system)에서 지식 베이스는 규칙으로 표현된다. 규칙은 다음과 같은 형식으로 표현된다.

IF RC_1 AND RC_2 AND , …..., AND RCn THEN CF

여기서 CF 는 조건에 부합되는 새로운 사실을 의미한다. 찾아낸 새로운 사실은 다음 규칙의 조건으로 이용된다. 즉 새로 찾아낸 지식은 또 다른 새로운 지식을 찾는데 이용이 되는 것이다. 여기서 CF 를 노드로 표현하고 적용되는 RC 를 링크로 표현하고 이와 같은 여러 가지 영향의 관계들을 연결하면 chain 을 얻게 된다. 이러한 규칙들의 집합을 그래프 구조를 나타낸 것이 추론망(inference net)이라 한다.[7]



<그림 2> 추론망 예

4. 추론망 자동 생성기법의 필요성과 선행 조건

4-1 선행되어야 할 조건

이러한 추론망 자동 생성 기법을 사용하기 이전에 먼저 수행 되어야 하는 작업들이 있다. 첫번째로 문제를 해결하고자 하는 시스템 영역을 설정한다. 두번째는 설정된 영역에서 일어날 수 있는 모든 단편적인 지식들을 수집한다. 세번째로 해결하고자 하는 대상을 수집된 지식들로 재정의 하여 집합으로 구성한다.

FD(Final Decision) : 찾고자 하는 목표

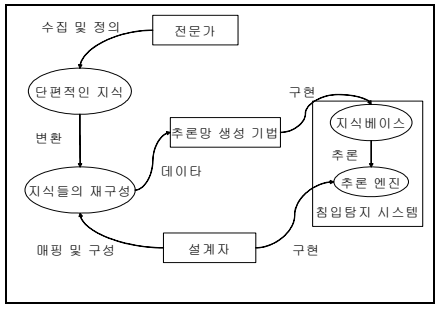
RC(Rule Condition) : 단편적인 지식들을 추론망 생성 기법에서 사용할 수 있는 정보 형태로 바꾼 조건들

CF(Create Fact) : 자동 생성 기법 중 생성된 지식들

CRC(Create Rule Condition) : CF 를 추론망 생성 기법에서 사용할 수 있는 정보 형태로 바꾼 조건들

4-2 추론망 자동 생성의 필요성

본 논문에서는 침입탐지 전문가들이 아는 단편적인 지식을 입력 받아 비정상적인 침입을 탐지하는 시스템에서 사용 할 수 있는 추론망을 자동으로 생성하여 추론을 모델화시키고 지식베이스화 시켜 비정상적인 침입을 탐지하는 방법을 제시하고자 한다.



<그림 4> 추론망 자동생성 기법을 이용한 지식베이스화 과정

5. 비정상 침입탐지 방법

5-1 추론망 자동 생성 기법

추론망 자동 생성기법이란 전문가들이 아는 단편적인 지식을 입력 받아 추론망을 자동으로 생성하여 추

론을 모델화시키고 규칙을 지식베이스화 시키는 기법이다.
자동 추론망 생성 기법의 알고리즘은 다음과 같다.
1.R 의 RC 와 CRC 이 포함하고 있는 R 들을 선택한다.
2.모든 R 들을 1 번을 같은 형식으로 선택한다.
3.연결이 없는 마지막 노드 들을 찾는다.
4.subtree-node 들을 찾는다.
5.찾은 subtree-node 들을 subnet 들로 구성한다.
6.branch-node 에 있는 delet-node 를 제거한다.
7.leaf-node 와 delet-node 일치하는 노드 제거한다.
8.root-node 나올 때까지 3~7 반복하여 수행 한다.
9.만들어진 subnet 들과 root-node 을 서로 연결하여 추론망을 생성한다.

5-2 비정상 침입탐지하는 추론망 생성

위에서 설명한 추론망 자동 생성 기법을 이용하여 비정상적인 침입의 탐지를 추론할 수 있는 추론망은 다음과 같다.

FD – SCAN, DOS, R-U 접근, 보안파일 접근, R 접근, 알려지지 않은 공격

rc1: Port Scan 공격이다.
rc2: OS 취약성 Scan 공격
rc3: Flooding 공격
rc4: Ping of Death
rc5: 무작위 대입법
rc6: Anonymous 접근 시도
rc7: User 보안파일 접근 시도
rc8: Root 접근 시도
rc9: 버퍼오버플로워 Root 접근 시도
rc10: 의심나는 User 접속
rc11: 의심나는 Root 접속
rc12: 의심나는 행위하는 해커의 공격
rc13: 정상적인 행위하는 해커의 공격

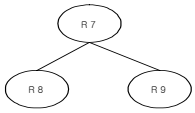
CF – SCAN, DOS, R-U 접근, 보안파일 접근, Root 접근, 의심나는 User 접속, 의심나는 Root 접속, 의심나는 행위, 의심나는 정상적인 행위

crc1: SCAN 공격
crc2: DOS 공격
crc3: Root_User 접근 공격
crc4: User 보안파일 접근 시도 공격
crc5: Root 권한획득 공격
crc6: 의심나는 User 권한 획득 공격
crc7: 의심나는 root 권한 획득 공격
crc8: 의심나는 행위를 하는 해커의 공격
crc9: 의심나는 root 의 정상적인 행위를 하는 해커의 공격

추론망 자동 생성 기법 알고리즘을 적용하여 생성된 모습은 다음과 같다.

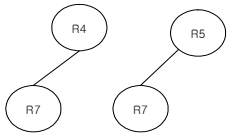
SCAN - crc1,(rc1 or rc2) -R1
DOS- crc2, (rc1 or rc2), (rc3 or rc4) -R2
R-U 접근-crc3, (rc1 or rc2), (rc5 or rc6) -R3
보안파일 접근-crc4, (rc1 or rc2), (rc5 or rc6) rc7, rc10 -R4
Root 접근-crc5, (rc1 or rc2), (rc5 or rc6),(rc8or rc9), rc10 -R5
의심나는 User 접속-crc6, (rc1 or rc2), (rc5 or rc6), rc10 -R6
의심나는 Root 접속-crc7, (rc1 or rc2), (rc5 or rc6),(rc8or rc9), rc7, rc10, rc11 -R7
의심나는 해위-crc8, (rc1 or rc2), (rc5 or rc6),(rc8or rc9), rc7, rc10, rc12 -R8
의심나는 정상적인 해위-crc9, (rc1 or rc2), (rc5 or rc6),(rc8or rc9), rc7, rc10, rc13, -R9

R1-R2, R3, R4, R5, R6, R7, R8, R9
R2-
R3-R4, R5, R6, R7, R8, R9
R4-R7, R8, R9
R5-R7, R8, R9
R6- R4, R5, R7, R8, R9
R7- R8, R9
R8-
R9-



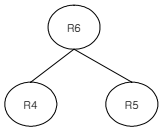
<그림 5> Subnet 구성

R1-R2, R3, R4, R5, R6, R7
R2-
R3- R4, R5, R6, R7
R4- R7
R5- R7
R6- R4, R5, R7
R7-



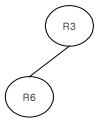
<그림 5> Subnet 구성

R1-R2, R3, R4, R5, R6
R2-
R3- R4, R5, R6
R4-
R5-
R6- R4, R5



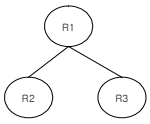
<그림 5> Subnet 구성

R1-R2, R3, R6
R2-
R3- R6,
R6-



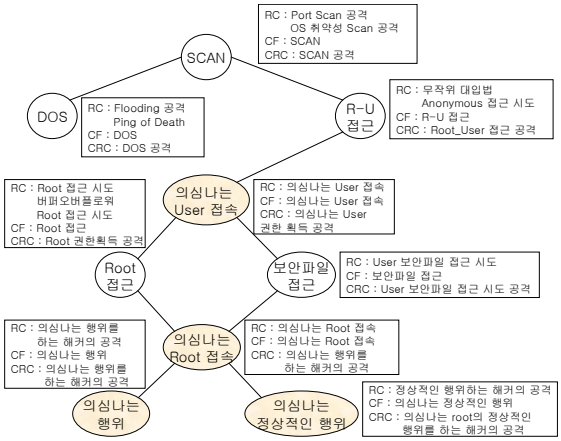
<그림 5> Subnet 구성

R1-R2, R3,
R2-
R3-



<그림 5> Subnet 구성

위와 같은 방법으로 추론망은 생성 된다. 최종적으로 생성된 추론망은 <그림 6> 와 같다. <그림 6> 에서 보면 User 의 접속과 Root 접속도 침입이라 추론할 수 있는 지식들을 기술하고 있으며, root 의 행위들도 침입으로 탐지하는 지식들이 포함되어 있다.



<그림 6> 최종 추론망 생성

6. 결 론

기존의 침입탐지 기법은 여러가지가 있지만, 모든 침입을 다 탐지하는 것은 것은 아니다. 비정상적인 침입을 탐지 하기 위해 여러가지 연구가 진행이 되고 있지만 아직 비정상 침입의 탐지를 현실화 하기에 많은 문제점이 발생하고 있다. 그래서 알려지지 않은 침입을 탐지하기 위해 전문가 시스템을 이용하고 패턴을 지식 베이스화하는 작업과 그 지식을 추론할 수 있는 추론망을 추론망 자동 생성 기법으로 구성하여, 비정상적인 침입을 탐지하는 방법을 본 논문에서 제시하였다. 이런 추론망 자동 생성 기법으로 만들어진 추론망은 알려지지 않은 침입을 침입으로 탐지하는 방법이 되면 전문가 시스템의 지식베이스로 적용하여 탐지를 할 수 있게 된다

추론망 자동 생성 기법으로 생성된 알려지지 않은 침입탐지를 하는 방법도 한계가 있다. 첫번째는 아직까지 지식 추출이나 지식 획득에 있어 전문가에 독립적이지 않다. 단편적인 지식 수집이나, 이런 지식의 매핑 집합을 구성하는 것들은 전문가 또는 개발자가 선택의 여부에 따라, 생성되어지는 추론망이 다르게 생성되고 탐지도 다르게 이루어진다. 두번째는 모든 비정상적인 침입의 탐지가 가능한 것은 아니다. 다른 새로운 취약성이나 아니면 톡특한 해킹방법으로 이루어진 침입은 탐지가 불가능하다. 그리고 추론망을 생성하기 위한 주어진 단편적인 지식의 정확성에 따라 탐지의 정확성도 문제점이 발생하고 있다. 세번째는 아직까지 실질적으로 알려지지 않은 침입을 탐지 해본 적이 없다는 없다는 것이다. 얼마나 실 세상에서 많은 오류 없이 침입을 탐지 할 수 있지는 미지수이다.

참고문헌

[1] John McHugh et al "The Role of Intrusion Detection Systems", IEEE SOFTWARE, 2000
[2] 한국정보보호진흥원, "침입탐지시스템 평가기준 해설서", 2001
[3] Stonebraker, M., "Implementation of Rule in Relational Database System," Database Enginering Vol.6, No.4 1983.
[4] Kellagg,C., "From Data management to Knowledge to Knowledge Management, " IEEE Computer, Jan.,1986
[5]김연만, dBASE III PLUS 한국컴퓨터매거진 출판국, 1993
[6] 이윤배,"전문가 시스템", 홍릉 과학 출판사, 1997, chap.4
[7] P. H. Winston, "Artificial Intelligence : The Third Edition", Addison Wesley, 1992 chap. 8
[8] http://myhome.hananet.net/~madeweb/es.html
[9]http://khic.kyunghee.ac.kr/kang/Lecture/khu_mis/class_rm/docs/ch_10/ch10-2.htm
[10]http://khic.kyunghee.ac.kr/kang/Lecture/khu_mis/class_rm/docs/ch_10/ch10-1.htm