2001년 한국정보처리학회 추계 학술발표논문집 제8권 제2호

N-code를 이용한 규칙 기반 침입 탐지 시스템

빙영태*, 차병래*, 서재현*
*목포대학교 컴퓨터공학과
e-mail:ytbing@songwon.ac.kr

Rule-Base Intrusion Detection System Using N-code

Young-Tae Bing*, Byung-Rae Cha*, Jae-Hyun Seo*
*Dept. of Computer Engineering, Mokpo National University

요약

최근 인터넷의 확산에 따라 여러 가지 침해사고 발생이 증가하고 있어서 시스템을 안전하게 관리하기 위한 노력들이 행해지고 있다. 본 논문에서는 NFR의 N-code언어를 이용하여 Shieh 모델의 침입 패턴을 탐지할 수 있는 규칙 기반 침입 탐지를 설계 및 구현한다. 제안하는 침입 탐지는 웹 기반에서 Shieh 침입 탐지 모델을 N-code 언어로 변환하여 침입 탐지여부를 쉽게 발견한다. 그리고 다양한 규칙들을 정의하고 이를 바탕으로 하여 취약점을 보완할 수 있도록 침입 탐지 시스템을 구현한다.

1. 서론

현재 컴퓨터 기술의 발달과 인터넷의 확산으로 누구나 쉽게 해킹 정보를 접하게 되고 다른 시스템에 침입할 수 있는 해킹이 늘게 되어 컴퓨터의 보안 문제가 심각하게 대두되고 있다. 최근의 보안 사고는 내부 및 방화벽을 통과한 침입자들이 대부분을 차지하고 있는 실정이므로 내부 시스템 보안이 중요시되고 있어 침입 탐지 시스템의 비중이 증가되고 있다.

본 논문에서는 NFR(Network Flight Recorder)의 N-code언어를 이용하여 허가되지 않은 사용자를 탐지하도록 하며 웹 기반에서 시스템의 침입 탐지 여부를 판단할 수 있고 모아진 데이터를 이용하여 최근의 네트워크 검색 공격 형태를 가장 잘 탐지하고 효과적으로 대응할 수 있는 침입 탐지 시스템을 구현하기 위해 NFR의 필터링 언어인 N-code를 이용하였다[1].

2. Shieh의 모델

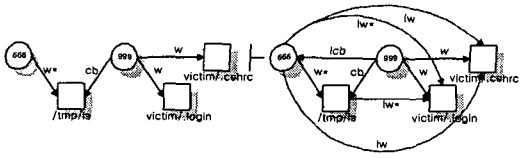
Shieh의 침입 탐지모델은 직접 관계(direct relation)에서 시스템 상태와 상태 전이, 주체와 객체 사이의 간접 관계(indirect relation)를 나타내는 규칙으로 정의된다.

시스템 상태는 정점의 집합으로 구성된 구조 V, 명명된 선분의 집합 E로 구성된 방향 보호 그래프 $G(V,E)$에 의해 정의된다. 정점의 집합으로 구성된 구조 V는 주체(○), 객체(□) 그리고 주체 또는 객체(⊠)로 구성된다. 방향성 있는 선분의 집합 E는 $e_i \in E$인 각각의 방향 선분은 순서화된 정점의 쌍의 원소를 연결한다. 심볼 * 은 과거의 단일 오퍼레이션이고 유한 관계 집합 $R = \{r, w, cb, d, I_r, I_w, I_{cb}, I_d, r^*, w^*, cb^*, d^*, I_r^*, I_w^*, I_{cb}^*, I_d^*\}$의 부분집합으로 명명된다. 보호 그래프는 주체와 객체라는 두 가지 타입의 노드를 가지고 있으며, 주체는 프로세스와 사용자들을 표현하는 능동적인 노드로서, 주체와 객체 사이의 데이터와 권한의 흐름을 발생시키는 행위를 초기화한다. 객체는 이와 반대로 수동적인 노드로서 파일이나 디렉토리와 같은 데이터 컨테이너(data container)를 나타내고, 데이터나 권한의 흐름과 같은 행위를 초기화시킬 수 없다.

상태 전이는 현재의 접근 연산들에 의해 결정된다. 시스템의 상태 전이는 현재의 관계들 $V \times A \times V$의 집합 L_c, $A = \{r, w, cb, d\}$ 그리고 예외 조건 결

과의 집합 D로 구성되며 $T: L_c \times G \rightarrow G \times D$ 와 같이 정형화되어 정의된다. 상태전이 동안에 침입 패턴이 발생되어짐을 결정하기 위해서는 시스템의 모든 간접 관계들이 유도되어져야 한다.

호스트 환경 하에서 시스템의 상태 및 상태전이 표현을 침입 탐지 보호 그래프로 표현하여 침입패턴을 생성하며 이러한 침입패턴이 침입인지 정상적인 수행인지를 검증하게 된다[2].



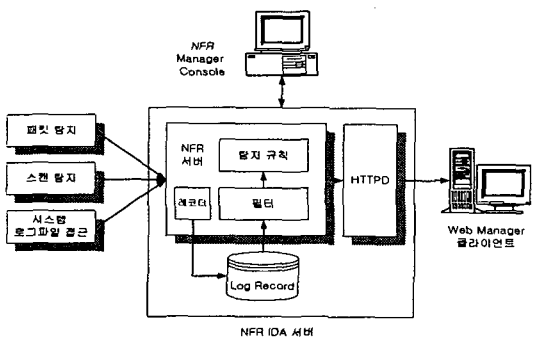
(그림 1) Shieh의 침입 탐지 모델

프로세서 666은 /tmp/ls라는 명령을 생성하고 프로세서 999는 /tmp/ls에 제어를 넘겨주므로서 /tmp/ls는 victim/.cshrc과 victim/.login을 변경하게 된다. 프로세서 666과 /victim/.cshrc과 victim/.login 사이의 간접 관계가 유추된다. 이 흐름은 다른 사용자들이 한 사용자의 중요한 파일에 직접적으로나 간접적으로 write하는 것을 금지하기 때문에 불법적인 것으로 정의하여 침입 행위로 간주한다.

3. 규칙기반 침입 탐지 설계

3.1 규칙 기반 침입 탐지 구성도

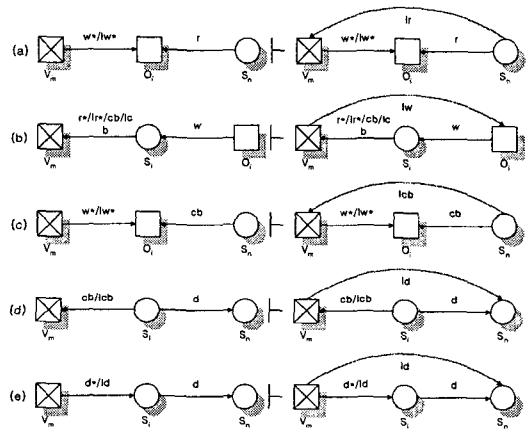
NFR Server에서 네트워크를 지나는 패킷이나 Unix, NT server의 시스템 Log를 받아 N-code에 의해 만들어진 규칙에 위반되는 데이터를 디스크에 저장한다. 본 시스템에서는 웹을 통하여 위치에 관계없이 시스템에 접근 권한만 있으면 어느 곳에서도 NFR 서버에 접근하여 새로운 규칙들을 정의하고 로그 분석 및 포트 감시, 네트워크 트래픽과 패킷을 분석할 수 있는 시스템을 구현하였다[3].



(그림 2) 규칙 기반 침입 탐지 구성도

3.2 간접 관계 탐지 규칙

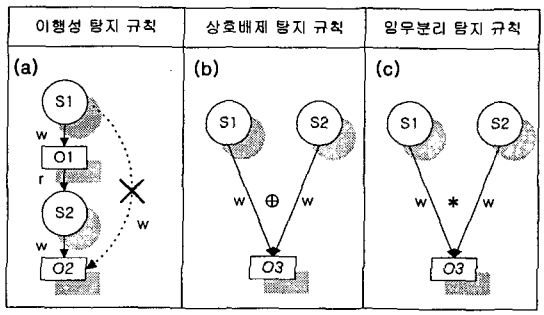
Shieh 침입 모델의 간접 관계를 탐지하기 위해서는 5개의 간접 관계 탐지 규칙을 (그림 3)과 같이 정의한다. 이러한 규칙은 주체/객체가 객체에 쓰기 연산을 수행하고 주체가 다시 읽기 연산을 수행한 시스템 상태를 표현한다. 이러한 상태는 오른쪽의 상태로 상태전이가 되는데 이는 간접적으로 주체/객체에 읽기 연산이 제공된다는 규칙이다. 예측 가능한 침입규칙 생성은 이상 탐지 기술로서 주체와 객체사이에 접근권한의 적용 순서는 임의적이 아니라 인식할 수 있는 패턴이라는 가설을 기초로 하고 있다. 이러한 규칙은 주체와 객체사이에 관계와 수행 순서를 고려하기 때문에 다른 침입 탐지 방법보다는 상대적으로 실시간 적이며 효율적이다.



(그림 3) 간접 관계의 침입 패턴 탐지 규칙

3.3 무결성 탐지 규칙

정보의 흐름을 통한 침입 패턴 탐지뿐만 아니라 무결성 유지 규칙을 제공하여 침입 패턴 탐지도 가능하다. 제안하는 무결성 탐지 규칙은 (그림 4)와 같다.



(그림 4) 무결성 탐지 규칙

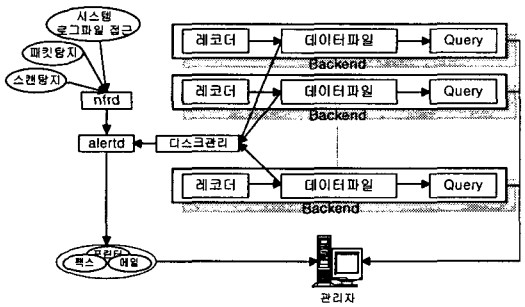
이행성 탐지 규칙은 임의의 상태의 특정 객체에 기록연산은 반드시 하위 상태를 통해서만 가능하다. 상호배제 탐지 규칙은 임의의 상태의 특정 객체에 기록연산을 수행하면, 그 상태에서의 그 객체에 대한 기록 연산을 수행할 수 없다. 임무분리 탐지규칙은 임의의 상태의 특정 객체에 기록연산을 수행하면, 그 상태에서 그 객체에 대하여 다시는 기록연산을 수행할 수 없다.

4. 규칙기반 침입 탐지 구현

4.1 NFR의 N-Code

N-code언어는 포로토콜 분석, 내용 검색/매칭을 수행할 수 있으며 오버플로우, Stealth 포트스캔, CGI 공격, 운영체제 확인 시도 등의 다양한 공격과 스캔을 탐지할 수 있는 필터링 언어이다. 또한 이러한 탐지 규칙들은 보안 Community를 통해 지속적으로 갱신되고 본인이 쉽게 규칙을 작성하여 추가할 수 있으므로 최신 공격에 적용하기 쉬운 언어이다.

N-code 언어를 이용하여 규칙을 만들기 위해서는 IP 헤더(ip 헤더 길이), TCP 헤더(tcp flags), UDP 헤더(목적지 포트), ICMP 메세지(메세지 유형) 및 시스템 여러 로그 파일들을 이용하여 규칙에 적용하여 침입 탐지 판별 및 데이터를 기록한다.



(그림 5) NFR 구조

4.2 침입 탐지 규칙의 N-code변환

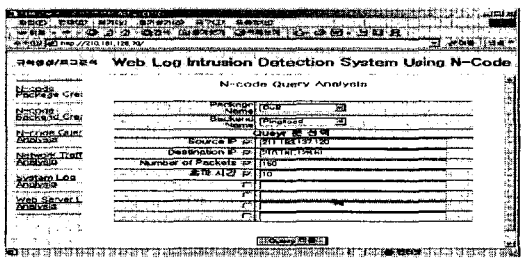
간접 관계 탐지 규칙에서 정의한 (그림 3)을 N-code로 변환한 것이다. (표 1)의 코드에서는 먼저 사용자 로그인을 체크한다. 그리고 SIGNATURES에 정의되어 있는 명령과 비교하여 그 명령과 일치하는 것이 있으면 먼저 디스크에 기록하고 관리자에게 경고 메시지를 전송한다. 다음으로 명령 뒤에 따라오는 인수들을 체크하여 그 인수가 BADARGLIST에 정의되어 있는 인수와 일치하면 디스크에 기록하고 관리자에게 경고 메시지를 전송한다. 마지막 줄에 있는 shieh_recorder는 shieh_schema에 정의되어 있는 폼에 맞추어 보고서를 만든다.

```
# Shieh rule
shieh_schema = library_schema:new( 1, [ "time", "ip",
        "int","ip","int", "str", "str","str"], scope() );
------[중간생략]-------
#사용자의 파일 읽기 체크
declare $login inside tcp.connSym;
  if ($login) {
    if (regexec(SIGNATURES,$cmd)) {
      record system.time, tcp.connSrc, tcp.connsport,
          tcp.connDst, tcp.conndport, "다른 사용자가
          명령을 읽음", $line,$username to
          shieh_recorder;
          alert(source_me,alert_shieh_cdbefore,
          alert_context_shieh, tcp.connsrc,tcp.conndst);
          return;
      }
      if ( index($arg, BADARGLIST) >= 0) {
        record system.time, tcp.connSrc, tcp.connsport,
        tcp.connDst, tcp.conndport, "의심가는 파일이나
        디렉토리", $line,$username to shieh_recorder;
        alert(source_me,alert_shieh_baddir,alert_
          context_shieh, tcp.connsrc,tcp.conndst);
        return;
      }
      return;
  }
------[중간생략]-------
}
shieh_recorder=recorder( "bin/list %c", "shieh_schema" );
```

(표 1) 간접관계 탐지규칙을 N-code로 변환한 것

4.3 침입 탐지 구현

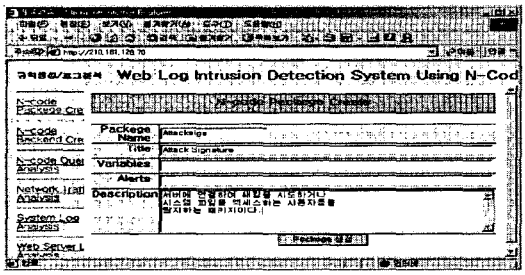
규칙 기반 침입 탐지 기법의 장점은 데이터나 특권의 흐름을 균일한 패턴으로 정의함으로서 안정성을 지원하는 시스템들에서 접근 권한의 오용을 막을 수 있다. 시스템의 여러 로그 파일과 히스토리 파일을 수집하여 (그림 6)과 같이 필터링하여 종합적인 로그 파일을 생성한다. 생성된 로그 파일로부터 간접 관계의 침입 패턴 탐지 규칙과 무결성 탐지 규칙이 변환된 N-code를 수행한다. 수행된 N-code에 의해 침입에 해당하는 침입패턴을 탐지하고 경고 메시지를 관리자에게 전송하고 침입패턴의 로그 데이터를 저장한다.



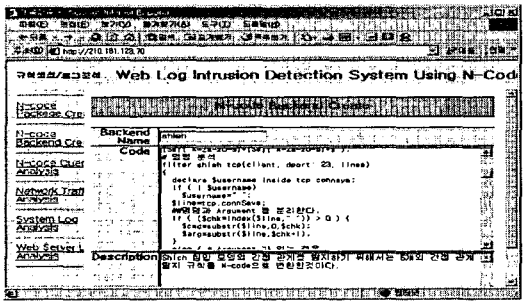
(그림 6) 로그 파일의 필터링

이 시스템은 N-code 언어를 이용하여 규칙을 정의하는 과정으로 (그림 7)은 패키지를 생성하는 화

면이고 (그림 8)은 침입 탐지 규칙을 생성하는 과정을 보이고 있다. 규칙들은 패키지라 불리는 그룹에 저장하는데 패키지는 backend라는 여러 탐지 모듈들이 적재되어 있다. backend는 NFR IDA의 기본적인 요소들 중의 하나이며 필터, 설정파일 그리고 기록기로 이루어져 있으며 기록된 데이터의 타입을 제어하고 기록할 수 있다. N-code를 이용하여 규칙을 정의해서 적용하면 NFR 엔진에서 규칙에 어긋나는 행위에 대해서 데이터를 기록하게 된다. 기록된 데이터는 필요한 데이터만 골라 분석할 수 있게 CGI 프로그램을 이용하여 구현했다. 패키지를 생성하는 pkginstall.cgi는 여러 backend를 그룹으로 만들기 위해 패키지 이름으로 폴더를 생성한다. 생성이 완료된 후 create_tables.cgi 프로그램은 (그림 8)에서 패키지에 해당하는 폴더에 탐지 모듈인 backend를 저장한다. nfrd 데몬은 패키지 그룹에 저장된 여러 탐지 규칙들을 작동시켜 규칙 모듈에 어긋나는 행위에 대해서 레코더 기록기에 보내어 로그 데이터 파일에 저장 및 alertd 데몬에 전달하여 관리자에게 경고 메시지를 보내게 된다.



(그림 7) 패키지 생성



(그림 8) 침입 탐지 규칙 생성

본 시스템은 침입 발생시 적절하게 탐지하였으며, BADARGLIST나 SIGNATURES 리스트에 해커가 시스템 권한을 얻기 위해 많이 사용하는 명령이나 인수를 추가하면 더 좋은 탐지 규칙을 만들 수 있다.

5. 결론 및 향후 연구방향

규칙은 주체/객체가 객체에 쓰기 연산을 수행하고 주체가 다시 읽기 연산을 수행한 시스템 상태를 표현한다. 이러한 상태는 간접적으로 주체/객체에 읽기 연산이 제공된다는 규칙이다. 예측 가능한 침입 규칙 생성은 이상 탐지 기술로서 주체와 객체사이에 접근권한의 적용 순서는 임의적이 아니라 인식할 수 있는 패턴에 기초로 하고 있다. 이러한 규칙은 주체와 객체사이의 관계와 수행 순서를 고려하기 때문에 다른 침입 탐지 방법보다는 상대적으로 실시간 적이며 효율적이다.

본 시스템에서는 여러 로그 파일과 히스토리 파일을 수집하고 N-code언어를 이용하여 종합적인 로그 파일을 생성하였다. 생성된 로그파일로부터 간접 관계의 침입 패턴 탐지 규칙과 무결성 탐지 규칙을 변환한 N-code를 적용하였다. 적용된 N-code 규칙에 의해 침입에 해당하는 패턴을 탐지하여 관리자에게 경고 메시지를 전송하고 침입패턴의 로그 데이터를 기록하고 사후 감사 기능을 수행한다. 수집되는 감사 데이터를 하나의 포맷으로 작성함으로써 침입 판정에 있어서 시스템 부하를 최소화하였다.

현재 시스템은 Shieh의 침입 탐지모델을 N-code로 변환한 규칙을 적용하였으나, 앞으로는 해커들의 비정상적인 침입을 탐지하는 비정상행위 탐지에서 침입 수법이 날로 변하기 때문에 자동화된 침입패턴의 업데이트와 침입 기법에 대한 연구가 필요하다.

참고 문헌

[1] NFR Security Inc., http://www.nfr.com/

[2] Shiuh-Pyng Shieh and Virgil D. Gligor, "On a Pattern-Oriented Model for Intrusion Detection", IEEE Transaction on knowledge and Data Engineering, Vol. 9, No. 4, July/August, 1997.

[3] Chad Childers & Linda Bangert, et al., "Tracking Web Usage with Network Flight Recorder", AACE, 1998.

[4] Judy Novak, Stephen Northcutt, et al., "Network Intrusion Detection An Analyst's Handbook", 2E, 2000.

[5] http://support.nfr.com/nid/docs/NID_N-Code_Guide.pdf